UNIVERSITY OF OSLO
Department of Informatics

Security aspects of OSPF as a MANET routing protocol

Øystein Larsen

1st November 2007

Abstract

This masters thesis deals with the security-related aspects of the OSPF routing protocol for use in Mobile Ad-hoc Networks (MANET).

OSPF, Open Shortest Path First, is an Intra-gateway routing protocol first developed as an IETF effort. It is widely adopted in large enterprise-scale networks, being well regarded for its fast convergence and loop-free routing. It is versatile in terms of which interface types it supports, such as point-to-point links or broadcast networks. It also offers scalability through hierarchical routing and by using centralization to reduce the amount of overhead on networks which have broadcast or broadcast-similar properties. An interface type missing from the standard so far is that of a wireless network, characterized by non-guaranteed bidirectional links combined with unreliable broadcasting, and existing interface types generally perform poorly under these networks. The IETF has therefore instituted a Working Group to standardize such an interface type extension to the latest version, OSPF version 3. This interface type will permit mobility and multi-hop characteristics in addition to those of wireless links in general. Such networks are usually referred to as Mobile Ad-hoc Networks (MANET). MANET routing protocols are subject to more severe security issues than ordinary, wireline-oriented protocols are. This thesis aims to assess and evaluate security of OSPF as a MANET routing protocol.

Contents

List of Figures

Acknowledgments

I extend my thanks to Dr. Eli Winjum and Prof. Leif Nilsen for their kind and knowledgeable assistance during work with this thesis, and necessary corrections during its final stages. This thesis was written with help from the Norwegian Defense Research Establishment (NDRE), and the author wishes to thank the GOSIKT project members for their support and contributions, both moral and professional, as well as for their hospitality and interest in my work. I would finally like to thank my patient family and loyal friends for their invaluable support and encouragement.

1 Introduction and background

Network routing is the process of receiving, analyzing and forwarding network layer datagrams, or packets, in a network. This is done by routers, network nodes that possess some information which allow them to make a decision on where to forward the packet next. In a small network of a stable structure, this can be done manually by the administrator, as the entire ARPANET was in its conception. The complexity of this task quickly passes outside of the boundaries of what is practically accomplishable as the number of nodes increases. This problem can be solved by letting the establishment of the pathways be an automated continuous process,carried out by the routers themselves.

The technical specification of such a process is a *routing protocol*. A routing protocol describes in detail both the underlying algorithm for determining optimal routes according to some metric, commonly called *cost*, as well as the exact bit-wise structure of the packets the routers will use. These packets serve the purposes of exchanging information useable for making packet forwarding decisions later, routing state. They also serve other purposes in the routing protocol, mainly various signalling between the routers. A set of routers that communicate to each other across one protocol reside in a common *routing domain*. Routing domains overlap and complement each other in accordance with boundaries determined by policies, topology and organization.

Efficient, stable and reliable routing is consequently of critical importance to modern computer network functionality. The routing process provides essentially the entire network layer connectivity of the network. An attacker intent on disabling or degrading the performance of a computer network would therefore be well served to explore the various possible means to attack the routing process. Such attacks can leverage inherent weaknesses of the protocol itself, or take advantage of illicit subversion of a router.

Routing security is the focus subject of this thesis. It is in short the study of the counterdefenses we would employ to make such attacks as difficult as possible. Provable security is not likely, because it usually demands costly and difficult formal modelling, while *strong* or *sufficient* security is a more attainable goal. Routing security research must employ the functional study of the routing protocol itself in order to uncover basic security threats in the way the protocol is designed. It must also identify which security services are needed to counteract such threats, and how to implement them. The network and link layers can potentially provide such services, and if so, the appropriate protocols must be chosen and adapted. This implies the more generic discipline of network security. Finally, the security of the router itself as a host must be adressed, often running a multi-user operating system.

1.1 Aim of this thesis

The aim of this thesis is to assess potential security threats to the OSPF routing protocol when used for wireless networks.

OSPF, in short, is an intra-gateway routing protocol (IGP) which is commonly used in medium-to-large networks. It supports a variety of network types by necessity, but so far lacks a standardized wireless interface type. Efforts are therefore being directed to adding such an interface type. This wireless interface will not only support wireless links, but also be adapted for use in Mobile Ad-Hoc Networks (MANET), which are [wireless] networks which offer continuous terminal mobility and multi-hop packet-forwarding, without a centralized infrastructure.

OSPF has a number of documented security vulnerabilities, of varying severity, and routing security researchers have also documented some of these through test-bed experiments. In combination with the security difficulties of operating in a MANET environment, there is a need to assess whether OSPF can operate securely in such an environment. Security protocols can offer end-to-end security between OSPF routers, but the protocols available may not be well suited to the needs of a routing protocol or the demands of a MANET. Therefore, the security protocols proposed should also be evaluated.

1.2 Contributions

The contributions of this thesis are highlighting security vulnerabilities in OSPF that are aggravated by introducing the protocol into a MANET. Furthermore, the scale of the damage of such attacks as demonstrated in wireline network testbed experiments combined with inherent properties of MANETs are used to illustrate the potential results of leaving these vulnerabilities unaddressed in the MANET interface type.

The IPSec security protocol is discussed as the standardized security service provider for the latest version of OSPF, version 3. The problems arising from using a one-to-one protocol to secure routing protocol traffic are addressed and explained, as well as the solutions the IETF has brought up to solve them. Last, the IPSec protocol is analyzed from the perspective of overhead and administration. Both perspectives see some substantial problems associated with IPSec. These are for the large part probably solveable, but the thesis cannot accomodate these solutions within its scope.

1.3 Methods

This thesis does not include simulated or testbed routing protocol attacks, for reasons of capacity and scope. By focusing on a small selection of attacks with their simulated or measured impact, the thesis would fall short of its goal of

providing a general-purpose assessment of the security aspects that arise from using OSPF in a MANET setting. The main issue is therefore not to show the possible extent of damage “Attack Y” can cause.

1.4 Structure

Sections 1.4 and 2.8 of the thesis describes and documents the OSPFv3 protocol as well as the suggested proposals for extending it with a MANET-adapted interface type. It is quite exhaustive, with emphasis being put on making the reader new to OSPF capable of understanding its functioning to a reasonable degree. OSPF is a quite extensive protocol, and while a good textbook is to be found for version 2 in [30], version 3 is mainly documented in terms of their mutual differences.

Section 3.9 describes the common security services, and attempts to create clear definitions of the concept of security in general in order to more precisely define routing security, network security and host security to provide more clarity. The section proceeds to describe the most central security services, all of which could be used by a routing protocol in order to attain security. The latter part of this section is devoted to IPSec, a security protocol suite intended to be used by OSPFv3 to offer end-to-end security services between routers. IPSec, like OSPF, is rather extensive. The section still has been made as short as the author believes is necessary.

Section 4.6.3 proceeds from Section 3.9 by further elaborating on the concept of routing security, with a focus on OSPF. It describes two main threat models - where the attacker/adversary works from, by what means, and with what capabilities. The motivation for this subsection is that having a clearly defined threat model set is a prerequisite to determine potential routing protocol attacks. It proceeds to look at work done by the IETF within routing security in general. However, throughout the section, security aspects of OSPF are the main issues handled.

The last section before analysis and concluding remarks is 5.9.2, in which attack types are described in detail. Attacks directly exploiting the way OSPF works are given priority, but more general attack types are also discussed.

The analysis of this thesis aims to combine the extensive background section on routing security, the OSPFv3 routing protocol, attacks against OSPF and routing protocols, and MANET routing protocols. The purpose is to conjecture firstly if the attacks against OSPF that are already known will be affected in effectivity by a transition to the new interface type. Secondly, IPSec will be evaluated for use as a security service provider for a MANET routing protocol. Security challenges to OSPF in the MANET setting are identified and discussed.

The concluding remarks sums up the findings of the analysis and background sections, remarking on the key issues and, where possible, providing suggestions for areas of further study.

2 OSPF Version 3

2.1 Introduction to OSPF

Standardization of OSPFv2 began in 1987 under the auspices of the IETF, in a designated Working Group which exists to this day. This development cycle was one of the first major efforts of the IETF, which until then had mainly supplied engineering and research advisory papers, and the first formal specification in the shape of a Request For Comments (RFC) document was released in 1991. The first version, OSPFv1, was intended for development purposes only, with the first (and current common) operational version being OSPFv2.

As OSPF was implemented by vendors and deployed, the experiences gathered led to improvements in the protocol specification. Towards the end of the decade, it was apparent that IPv4 would not be a sustainable network layer protocol in the long term, and to accomodate the new IP version as well as greater changes to the protocol deemed beneficial which was outside of the scope of RFC revisions, the OSPF working group began working on a new version.

Finally, a standard for OSPFv3 was first presented in December of 1999 in RFC2740 [10] by the IETF Network Working Group. It is, for the most part, similar to OSPFv2, documented in RFC2328 [31], in modes of operation, except where applicable due to IPv6 being assumed to be the networking protocol which it operates on. Therefore, RFC2740 mainly consists of establishing differences from OSPFv2, though in all cases, care must be taken when researching the finer points of OSPFv3, as there still are numerous differences between the two, and most literature available covers version 2. This can make understanding OSPFv3 tedious, as merely reading the RFC, intended for developer reference more than concise understanding, is inconvenient at best.

In order to determine and assess the security-oriented issues of OSPF in a role as a MANET routing protocol, we will need to have a solid basic knowledge of how the protocol operates, before moving on to the suggested improvements encompassed by the term OSPF-MANET. The following section provides the most necessary OSPFv3 [10] background to analyze OSPF-MANET strong and weak points from a security perspective.

OSPF-MANET does not constitute a complete rewrite of the protocol, and less so than OSPFv3 - OSPF was designed from the start to be versatile to ensure wide adoption in networks that increasingly were composed of different networking technologies other than the leased point-to-point links of the ARPANET. Network types are represented in OSPF by the type of each *interface*, of which four are defined in OSPFv3. Adding support for the peculiarities of MANET networks (multi-hop, non-reliable broadcast) is therefore a question of defining an interface type that precisely matches these networks and add mechanisms to this interface type which will offer the core link-state protocol the services (reliable flooding) it requires.

The main motivation for creating OSPF version 3 was to accomodate IPv6. However, this does not merely encompass fitting the longer adresses into the protocol headers. IPv6 differs from IPv4 in crucial points, notably the replacement of the IPv4 *subnet* with the IPv6 *link*, and the removal of the authentication header. Also importantly, OSPFv3 addresses the need to partition a link according to separate OSPF processes, or *instances*. Other changes are more subtle, but as security often hides in the details, no less noteworthy, at least at a glance.

OSPFv3 does not identify routers using IPv6 addresses, instead substituting them entirely for OSPFv2 32-bit Router IDs. The introduction of Link Local Adresses in IPv6 meant that the concept of *flooding scope* of packets, where to forward which types of packets, was put into effect. Where OSPFv2 only supported one running OSPF process per network, OSPFv3 adds the concept of the *instance*, which allows several running OSPF processes to share a link (IPv4 subnet). Finally, OSPFv3 is extensible in its header processing, like IPv6, by allowing for deeper processeing of unknown packet types. All of these features will be discussed in-depth and analyzed for security.

OSPF is a large and complex protocol. While in-depth knowledge of it is a necessity to assess it from a routing security perspective, there is the risk of loosing sight amongst the finer details of it. Where possible, these should be deferred until they become important to the subject matter at hand, i.e. whenever they are crucial to some routing security aspect of the protocol, to avoid losing perspective amongst the details.

2.2 Overview

OSPF is an *Interior Gateway Protocol* (IGP) intended for establishing routing tables, or *link state*, between cooperating routers operating inside the administrative confines of an *Autonomous System* (AS), alternatively called a *routing domain*. The proactive establishment of routes contrasts it with reactive routing protocols. In the latter, a route between two hosts is established on a per-request basis, usually with the possibility of some limited caching.

OSPF, as a true second-generation routing protocol, supports several network types apart from the conventional serial-line, point-to-point network of the Arpanet. However, other network types are also allowed, with the major divide being whether the network type supports broadcast or not. An OSPF router is configured with one or more *interfaces*, and, in the case of OSPFv3, *instances*. These network interfaces map to specific network types; host-to-host or point-to-point, broadcast, non-broadcast but with multiple medium access and point-to-multipoint.

The heart of OSPF is a *shortest-path first* (SPF) graph traversal algorithm known as Dijkstra's algorithm. This algorithm can create pathways in weighted graphs with the minimum weight efficiently. These pathways - essentially telling

the router where to send a packet next if it is destined for any given host - are stored as a routing table. It is easy to see how a network can be abstracted as such a graph, with the weight on each vertex representing some concept of cost, usually time or amount of hops. The actual implementation of Dijkstra's algorithm is rather easy, and can easily be done by a CS junior student with a basic course in algorithms and data structures. The algorithm cares in no way about the type of network from which the information is gathered, that is, what interface (link) type it is gathered from, not about the quality of the data fed into it, so it has no security perspective.

The question of OSPF security is, in short, mainly concentrated in the part of the protocol which disseminates and receives information it feeds into this central algorithm - information gathered from and shared with the other protocol instances with which it communicates. This topic will be more thorougly adressed in Section 4.6.3, with some background material on routing security in general being available in Section 3.9

The network information gathered by the protocol interfaces and processed by the graph traversal algorithm is finally stored in the basic data structure of OSPF, the *link state database*, a complete network topology table which permits routers to know the ID of all routers inside the domain, which routers have a direct link to which, how many interfaces each router operates, and cost. Cost is currently not in active use by industry vendors, preferring other means to calculate the cost of a link for management and tallying purposes. The link-state database is maintained and exchanged to new routers by *link state advertisements* emitted periodically.

Each LSA is transmitted using a technique called *reliable flooding*, which implies that all routers in the routing domain/AS is guaranteed to receive the LSA. The manner in which reliable flooding is achieved is dependent on *interface type*, the type identifier that determines which link type a router interface ("network card") is connected to and upon which OSPF makes assumptions about broadcast capability and media access.

OSPF transmits packets directly over IP, as opposed to using TCP, UDP or other transport protocols. The OSPF payload is contained directly within the IP datagram. The lack of a dedicated transport protocol to ensure reliable end-to-end transmission required OSPF to ensure reliable flooding of OSPF information by other means.Importantly, IPv6 offers OSPF the option of taking advantage of the security services offered by IPSec; more on the latter follows in later sections. Why does OSPF not use UDP or TCP, or even the link layer, to encapsulate its packages? To address the latter first, link layer protocols like Ethernet do not offer fragmentization of packages, consequently OSPF would need to implement fragmentization mechanisms by itself, complicating and slowing packet ingress and egress. In addition, to correctly perform fragmentization with varying link layer protocols, OSPF would have had to establish a set of link layer identifier classes that determined which link layer frame length would be used. As for TCP and UDP, the advantage TCP offers ahead of UDP is the ability to reliably deliver

packets on an end-to-end connection. However, OSPF itself uses mechanisms, depending on network (interface or link) type, to ensure that packets are flooded reliably. Likewise, to ensure TCP flooding, each router would need to establish a TCP three-way handshake with all corresponding routers on the flooding network. This would introduce unnecessary overhead for functionality that already exists. UDP being the remaining candidate transport protocol, was found to offer few advantages that OSPF truly needed. Additionally, on most systems, a UDP socket is available to most or all users. Sending directly over IP, however, is usually a privilege of root- or system accounts, denying average users the possibility of sending OSPF packets, which was seen as a security benefit.

OSPF allows for hierarchical routing, dividing the network into two strata, the higher of which is a "common" or "backbone" across which information is disseminated between the lower. If used by the network administrators, this hierarchy permits a network running OSPF to grow without the complexity of the routing information exchange growing exponentially along with it. Thus it permits scaling.

On multiaccess networks, which unlike the point-to-point links link state routing was originally conceived, the routers will either themselves elect (broadcast) or be configured as (non-broadcast) a *Designated Router*, DR. The DR adds scalability further by centralizing the processing of link state databases, instead of each router carrying out the CPU- and network-costly process itself.

2.3 IPv6 issues relevant to OSPFv3

This subsection details those parts of the IPv6 protocol which affect OSPFv3. This includes issues both pertaining to operation, as well as security. However, the former is the focus of this part of the thesis, hence any references to IPv6-related security issues will be postponed until needed.

IPv6 is a development of the IPv4 network protocol component of the TCP/IP network stack. IPv6 is intended to replace IPv4, coexisting alongside it for a period of time using tunneling, while vendors and users are re-configuring their networks and sunsetting legacy systems. IPv6 is mainly known for solving the address space problems of IPv4, alleviated with NAT and classless addresses, but it also offers other improvements - most important of which for the relevance of this thesis is that IPSec, an end-to-end set of security protocols, is mandatory in IPv6, whereas it is electable under IPv4. IPSec is described in detail in a separate section.

Until 1993, IPv4 used a system known as *classful addresses*, which separated IP-addresses into five classes spanning from A to C (with D and E being multicast and broadcast addresses) depending on how many "free" bits were in an address assigned to a network. For example, class A networks, the largest, were addresses in which the leading eight bits were network identificators leaving the remaining 24 bits free for individual hosts, with a total of $2^{32} - 2 = 16'772'214$ addresses available in the network. Since this implied a large amount of wasted addresses,

and a maximum amount of networks of 256 in all (including classes A, B and C), the IETF left the concept of classful addresses behind. The system which replaces classful addressing is the one which also introduced the concept of subnetting to IPv4: CIDR, *Classless Inter-Domain Routing*. CIDR divides addresses according to a more flexible scheme than classes do. Instead of operating with class hierarchies in which bits are free in divisors of eight, classless addresses can set any number of bits free. Hence, the address 129.240.2.3 could now belong to a network designated 129.240.2/ which excluded 129.240.2.214, whereas both would have to be a member of the same C-class network previously. Consider the following table showing this mask and two addresses:

	Sub-network address	IPv6 addres range
Mask	129.240.2.8/3	10000001.11110000.10.00001$\{b_1 b_2 b_3\}$
A	$129.240.2.15_{10}$	$10000001.11110000.10.00001111_2$
B	$129.240.2.214_{10}$	$10000001.11110000.10.11010110_2$

A matches the mask, while B does not.

The subnetting concept is itself an abstraction. By this is meant that it is a method in which to organize networks into zones and hierarchies not mandated by or reflections of some basic property of IP addressing. As far as the link-layer directly beneath IP, in whichever form it may be, is concerned, choosing what frames to forward is merely a matter of medium connectivity. Therefore, another approach to viewing subnets might be to make the link layer reflect itself in the network-layer protocol. To avoid a breakdown of the barriers between network layers, the IPv6 protocol adds support for the concept of the link layer in the shape of the *link*.

An IPv6 subnet is essentially a contiguous interval of addresses. This interval must be of a size on the form 2^n. The relationship between links and subnets is that the link is encompassed by the subnet, and that several links can be contained in a subnet.

In short, links in essence are an abstraction of the link-layer protocol services.To quote RC2460 [11]:

> link - a communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IPv6. Examples are Ethernets (simple or bridged); PPP links; X.25, Frame Relay, or ATM networks; and internet (or higher) layer "tunnels", such as tunnels over IPv4 or IPv6 itself.

An Ethernet network running OSPFv2 will offer the same broadcast “scope” to all hosts connected to it regardless of addressing semantics. This concept of “broadcasting scope” or “link scope” is reflected in some crucial changes from OSPFv2 to OSPFv3, detailed further in this Section. Section 2.5.3 illustrates and

elaborates on the link concept as it relates to routers in particular. The implications it has for addressing is discussed here, however, since OSPF routers do not use IP addresses in the "overlay net" the routers are members of.

IPv6 addresses that are valid only inside the link broadcast scope are referred to as Link-Local. Link-Local IPv6 addresses are not used for routing purposes, but are used for more temporary purposes: neighbour discovery, and in an infrastructureless network, they are used for stateless autoconfiguration (i.e., the host assigns an address to itself) allowing for temporary networks where only connections between hosts is of interest. They are always preceded by the address prefix `FE80`. For reference, the equivalent class of these addresses in IPv4 are for instance the 192.168/16 and 10.0/16 subnets. A related concept is the *unique local IPv6 unicast address*, usually merely referred to as "local IPv6 addresses", previously known as site-local addresses. Preced by the address prefix `FC00`, these addresses define networks whose addresses are non-routable globally, like link-local addresses. Examples of usage may be sensor networks in a factory.

OSPFv3 no longer uses any addressing in its headers - all "OSPF adresses" are in fact 32-bit router IDs, and routers only know each other by these IDs. This actually means that OSPF is essentially independent in its operation of the network protocol it runs across - of course, several allotmens in OSPFv3 accomodates IPv6, but addressing is not crucial. The actual link state, of course, still consists of IPv6 addresses.

2.4 Central concepts and components

The following section introduces central concepts of OSPF and Link State routing. It does not need to be read in order as a block to understand the sections it precedes, but is rather intended to serve as a point of reference for whichever central concept of LS routing the reader is not familiar with or where doubt arises on the use of terminology. The Terms and Abbreviations section at the end of the thesis may also be useful.

2.4.1 Interior and Exterior Gateway Protocols

An Interior Gateway Protocol is a routing protocol designed to operate inside an Autonomous System 8. The complementary protocol type is that of the Exterior Gateway Protocol, which consists of those protocols intended to establish routes between Autonomous Systems. The main example of the latter is BGP. Interior and Exterior Gateway Protocols exchange routing information depending on the design of each protocol. In an OSPF AS, this exchange is handled by Autonomous System Border Routers (ASBR).

2.4.2 Link State Routing

Link state routing was invented in the late 1970s at Bolt, Beranek & Newman (BBN). The ambition of the inventors was to provide a more stable routing service in a network than previous manual routing protocols permitted. Later work at BBN with Link state routing led to the invention of hierarchical Link state routing.

To say that a routing protocol implements Link state routing, implies that the router running the protocol has complete knowledge of the entire routing domain. This knowledge is exchanged between routers in the shape of Link state, which is a unit of information describing a shared Link between two routers. This information is collected in Link State Advertisements (see below).

The Link state is aggregated by each router, as a list or database. The Link state is then used to establish all possible routes in the routing domain in the shape of a routing table generated with a Shortest Path First algorithm. Routers can obtain the link state by means of interaction with other routers, either by receiving and broadcasting periodically emitted messages containing Link State Advertisements, or alternately, by obtaining the full Link state of a neighbouring router, in the case of OSPF, by means of Database Descriptor packets. The latter is used when a new router is discovered in a network.

2.4.3 Distance Vector Routing

Distance Vector routing differs from Link State routing in that routers exchange actual routing table information instead of merely the Link state used to generate it. To elaborate; each Link state router creates its routing table by its own internal processes. The Distance Vector protocol, on the other hand, keeps Link state local at each router, and propagates routing tables.

Even though OSPF is considered a Link State protocol, it does in fact also use Distance Vector routing in implementing hierarchical routing.

2.4.4 Link State Advertisement

Link State Advertisements are the OSPF link state data units. They are of a fixed length. While coalescing LSAs could offer more efficient handling and transmission, practical experience by the implementors of the original OSPF protocol dictated that they be kept small. Each LSA contains a set of information detailing who originated it, its age and sequence number, and the actual link state, for example in the shape of a route offered by the originating router or the summary of a network. The LSAs are kept in a database ordered according to their unique identifiers. The link state contained in them is used by the router in its SPF calculations.

LSAs are flooded encapsulated in Link State Update packets. The flooding is ensured by a Link State Acknowledgement. They can be used to synchronize

the link state of one router with another, on a per-request basis, after the giving router sends a series of Database Descriptors to the receiving router containing information about which LSAs it keeps in its database.

Since the structure of LSAs is important to routing protocol security, as they are the prime vector through which harmful information can enter into the routing process, they are described in closer detail in Section 2.6.1.

2.4.5 Flooding and neighbor discovery

Flooding a message is, in essence, to re-transmit an incoming packet across all active interfaces, usually barring the incoming interface. Flooding can be achieved on all Link types, however, unicast flooding is rather inefficient compared to broadcast and multicast. By each recipient acknowledging receipt of the flooded packet, the sender can verify if the flooded packet was received by everyone. In OSPF, the Link State Ack2.7.2 is used for this purpose.

In essence, this replicates the functionality of a TCP-type connection-oriented transport protocol. Messages are forwarded on all interfaces, unless those on which they already have been received, and acknowledged back to the originator in the same manner. Flooding can either be carried out by means of broadcasting, multicasting or even by unicast. Flooding is the mechanism which allows routers to discover each other, exchange routing information, and notify other routers of changes. Flooding which can be guaranteed - all routers receive the message - is said to be *reliable.*

Reliable flooding is the means used to achieve certain delivery of these messages. The simplest way to describe this process is simply that the router originating the message to be flooded transmits is to each of its neighbors, who then transmit further out except on an interface on which the message has been recorded as arriving. Finally, each recipient acknowledges the receipt if an acknowledgment has arrived on each of the interfaces on which it has sent the message. The procedure may seem wasteful, but by tuning the interval before a router forwards each packet, the overhead redundancy can be trimmed.

On link types without broadcast, neighbour discovery must be carried out by manual configuration, and are maintained using unicast HELLOs.

2.4.6 Adjacency

Two OSPF routers that mutually synchronize their link state, form an *adjacency* with each other. On interface types such as point-to-point, the adjacency follows the single link between the two hosts. In other network types, where routers share the medium but are not capable of sending messages to everyone at once, adjacencies can be configured manually.

In a broadcast network, in which routers are self-configuring, a router arriving in the network that announces its presence, upon completion of initial link state

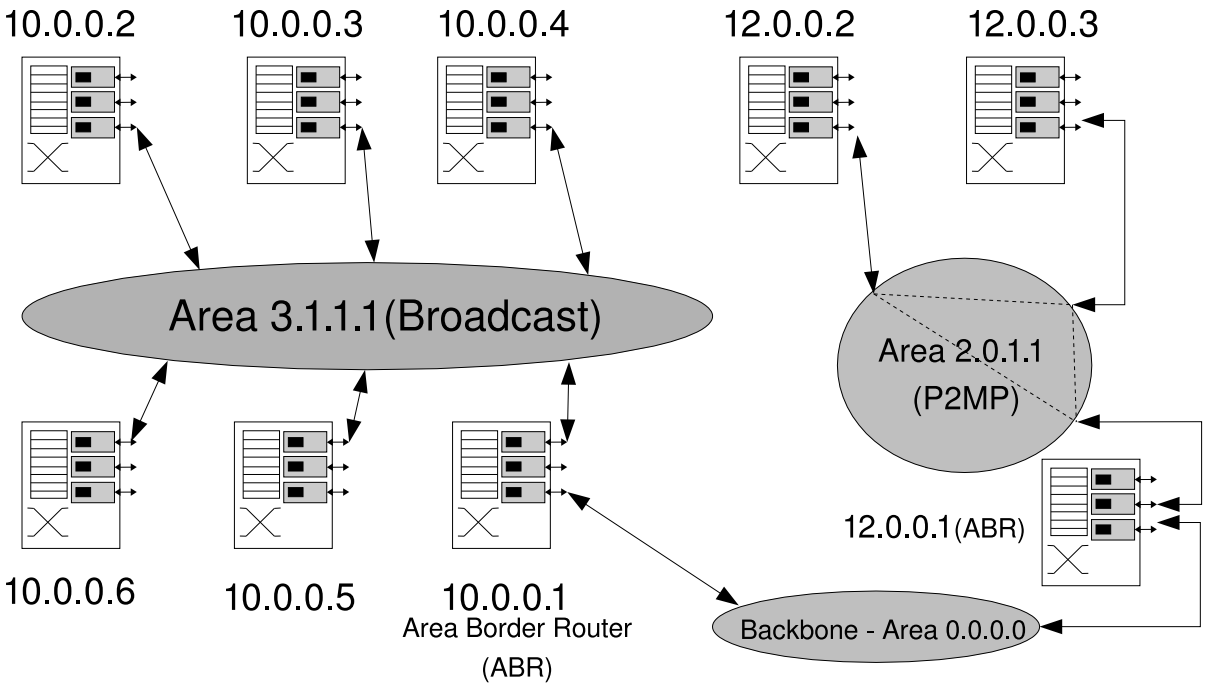

Figure 1: A simple illustration of the OSPF Area system

database synchronization, is said to be *fully adjacent* with the neighbor router from which it received the link state. Once full adjacency has been established, the new router will participate in updating the link state of other routers with *Link State Update* packets. The adjacencies can then be thought of as logical network paths across which Link State Updates and other OSPF control messages are shared. They form a separate meta-network distinct from the IP network it uses for transmission; OSPF transmits its information as 'raw' IP datagrams, and does not use any higher-level transport protocol. It is easy to see that the complexity of the amount of overhead traffic associated with link state updates approaches $O(n^2)$ with n being the number of routers. To alleviate this problem, OSPF permits activation a *Designated Router* scheme, either self-configuring in a broadcast network or manually configured in a non-broadcast network.

2.4.7 Areas

For purposes of scalability, the AS may be segmented logically into *Areas*, of various types according to their connectivity. For a simple illustration of Areas in a small network, see Figure 1. Area types are determined according to of which degree each Area is directly connected to other Areas and external Autonomous

Systems. Each Area receives a distinct 32-bit number identifying it. The Area mechanism thus introduces a notion of a two-tier hierarchy into the network. This allows for link state complexity on the order of $O(log(n)$, where n is the number of Areas, instead of $O(n)$ (linear complexity). Inside each Area, OSPF works as a link state protocol, with each router maintaining full state of the entire Area. However, between Areas, OSPF forwards link state in a fashion more resembling Distance Vector routing. This surprising fact lies in the Summary LSAs that are exchanged between Area Border Routers. The structure and origin of these closely align with how RIP builds routes [30]. It is for this reason that there may only be one backbone Area - with more than one, there would be several redundant paths, which could hurt DV convergence, in particular by making the count-to-infinity scenario possible. However, with the Backbone forming a hub between all Areas, this is effectively prevented.

The size of Areas can vary considerably between the recommendations given by vendors; establishing link state for an Area has complexity$O(i * log(n))$, where i is the number of interfaces and n routers, and essentially the number of routers in an Area is mainly constrained by the memory and CPU of the routers in it. An Area of 500 routers is not unheard of, but the recommended number can dwindle to as low as 50. [30].

The Area of central importance is the *Backbone Area*, always designated as number 0. Every Area-segmented OSPF network is built around this backbone, over which routing information is dissipated between routers in all the Areas of the Autonomous System. All Areas need to have an interface to the Backbone in a correctly configured OSPF network. If the Backbone Area cannot physically connect directly to an Area in the AS, a *Virtual Link* can be configured through another Area in order to reach it, acting as a packet tunnel. Virtual Links are regarded as Areas in their own right.

The typical area, in [30] simply called Normal Area, can be placed anywhere within the AS. This standard area type handles all LSA types, which can be a liability if one wishes to lower the amount of routing traffic overhead to a minimum in a dedicated Area. For this reason, three other Area types have been implemented that allow for more narrow link state propagation, reducing processing and link resouce usage.

These other three Area types apart from the backbone, normal areas and Virtual Links, are SA, TSA and NSSA, respectively meaning *Stubby Areas*, *Totally-stubby Areas* and *Not-so-stubby Areas*. Each is described in terms of their connectivity to other Areas or other Autonomous Systems. Dividing each Area is one or more border routers, described below.

The Stubby Area offers no routes that are not OSPFv3-generated routes, as it is connected to OSPF areas only, effectively meaning that any packet originating from a host inside the Area intended for an IP address outside of it, will be transmitted on the default, or “last-resort”, route. A Stubby Area will receive routing information

from other OSPFv3 Areas from the Backbone. It is the Area type which demands the least in terms of memory and CPU of its routers, hence LSA packets from outside the AS are not forwarded into the Stubby Area. A Stubby Area therefore cannot provide Virtual Links through itself, and so must be placed as "leaves" on the Area map.

Conversely, the Totally-stubby Area does not receive or transmit any routing information to or from other Areas. Its only external route is the default route. This austerity puts constraints on the forwarding delays of packets originating in this Area, making it an Area type that is only used when overhead in link and memory must be kept at an absolute minimum.

A slight extension of the Stubby Area, the Not-so-stubby Area can receive, and propagate to the Backbone Area, *some* routing information from other external Autonomous Systems. This permits the NSSA to receive routing information for example from an RIP domain through an ASBR at its boundary and propagate this further into the OSPF AS. However, the NSSA like the SA and TSA still cannot support Virtual Links through it.

The Area scheme of OSPF is complex. Its advantages, though, are indispensable: they provide the possibility of a hierarchically ordered network, where only the routing information necessary for each Area is broadcast within it, but at the price of a reduction in optimality of packet routes. As network size increases, this leads to a significant reduction in network overhead in total, while delays are considered an acceptable trade-off. Combined with the Designated Router scheme and the wide support of different interface types, this makes OSPF an adaptable and versatile protocol, as its wide adoption is further testament to. There are also other advantages: robustness increases as link failures or router faults are contained within each Area, the tendency to prefer intra-Area routes adds to this robustness. Additionally, since the Summary LSA can be configured to hide IP address ranges, subnets/links can be closed off to other Areas for security reasons.

OSPF at the inter-area level works, as mentioned, in a fashion similar to Distance Vector routing2.4.2. The basic cornerstone is the Summary LSA, described in detail further below. In short, the Summary LSA contains the ID of the originating router, and an IP address range and netmask detailing the addresses that are assigned to the Area the router represents.

2.4.8 Virtual links

Virtual links might be referred to as extensions of the Backbone Area across other Areas. It guarantees that the backbone will be contiguous even if it is not physically contiguous.

2.4.9 Router types

Routers in OSPFv3 are categorized as *AS boundary routers* (ASBR), *Area border routers* (ABR), and *internal routers*. Internal routers are only connected to one area, whereas Area border routers and Autonomous System border routers respectively maintain connections to several areas, and several Autonomous Systems. The ASBR is particular in that it can process and introduce link state received from non-OSPF protocols, in effect usually BGP (Border Gateway Protocol), the routing protocol that essentially connects the Internet.

Area border routers may also be specified as backbone routers, connecting it to other backbone routers, although this implication doesn't go the other way: a dedicated backbone router may exist which is not an Area Border Router.

Routers form specific relationships with each other, determining the activity between them. The "two-way" neighbor state indicates that a Hello packet has been received in both ends, marking a mutual discovery. The "exchange" and "full" states are used during and after initial database synchronization, respectively, while a missing "Hello" packet will result in a "down" state.

2.5 Links, interfaces and flooding scopes

The three above terms, already mentioned in various contexts, deserve a more thorough treatment on their own. They are related to each other in a sense which greatly influences how OSPFv3 accumulates, dissipates and organizes link state.

2.5.1 The interface

In OSPFv2, an *interface* is a logical assembly of a physical network adapter, an adress range, various transmission parameters such as Minimum Transmission Unit size (MTU) and Hello interval, Area type, Designated Router ID, and the interface type and state. The state can for instance be up, down, or loopback, while the interface types are described below.

The interface type describes the characteristics of the network the interface connects to. As mentioned, the OSPF-MANET strives to standardize an interface type that matches this kind of network in which the medium offers multiple access and unreliable broadcasting due to the nature of wireless communications. The most common interface type is broadcast2.5.3. Other interface types have little impact on this thesis and will only be mentioned briefly. It is worth noting that a MANET-enabled OSPF implementation will also support these other interfaces.

The interface type is important for the way the OSPF instance operates - across an NBMA interface, for instance, HELLO messages will be transmitted to each router on the interface in turn instead of multicast. This necessitates a longer HELLO interval. Conversely, a Broadcast type interface will see more frequent HELLO emits.

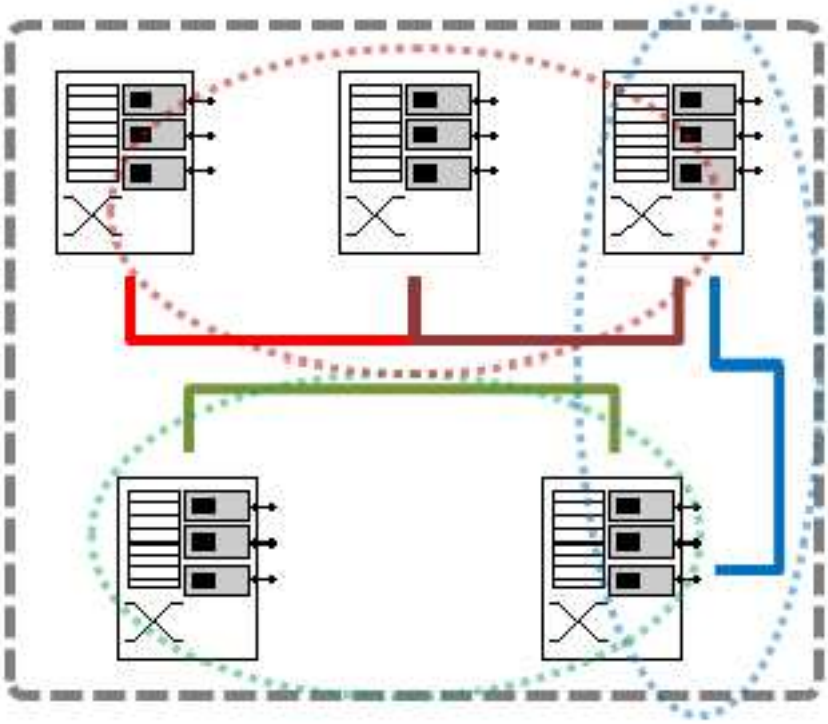

Figure 2: The relationship between Links and Subnets in IPv6

2.5.2 Instances

OSPFv3 elaborates further upon OSPFv2 by adding support for multiple *instances* for each link. The result of this is that a broadcast link, for example, may support several routing domains. A typical case could be two sets of routers that separately form two routing domains (Areas) while at the same time sharing the same Ethernet network. The routers differentiate between instances by a 32-bit integer contained in the OSPF header. The alternative to this scheme would under OSPFv2 be for instance to set authentication keys differently for each Area - but this is a hack at best, since all routers constantly would be logging failed authentication attempts.

2.5.3 Links

In short, the interface connects the routing process with a network, or, more precisely, a subnet. OSPFv3, operating under IPv6 with its addressing scheme, consequently dispenses with the subnet terminology from interface descriptions, replacing it with IPv6 *links*. A link, as described in the IPv6 subsection, is one or several subnets which share a common medium, broadcast or not. The relationship between areas and links is not necessarily one-to-one; a link may for instance belong to two OSPF areas, should this be desired.

Figure 2 shows the relationship between links and subnets. Five routers share four mutual links within the confine of one Area. These four links map to three distinct subnets within the Area.

The introduction of the link semantic to OSPF has necessitated a new type of LSA, the Link LSA. This LSA serves the purpose of neighbour discovery on the link, alerting other routers about which IPv6 address prefixes associated with the link, and it provides Option bits used for the Network LSA.

Links (or interface) types are assigned according to the properties of the network, with the same types retained from version 2 to 3. These are each given their own sections for completeness, since they vary widely in how security is concerned.

2.5.4 The broadcast link

The defining feature of a subnetwork (Area) to which the router interface is set to the *broadcast type* is that a packet emitted on that interface will be heard by all hosts on the subnet. The broadcast feature is therefore a function of the link layer being able to filter packets with specific link layer addresses from those with a specific broadcasting address. On Ethernet, this address is simply the highest possible 48-bit hexadecimal number (0xFFF...). An Ethernet adapter will accept packets with either its own or the broadcast address. Additionally, some networks and notably Etherner use a third addressing method, multicast, in which interfaces are programmed to accept a specific subgroup of addresses, enabling the possibility of defining "groups" of interfaces. Ethernet defines two such adresses relevant for OSPF, "AllSPFRouters" and "AllDRouters".

2.5.5 Designated routers

An important concept in OSPFv3 link types which permits more than two routers on the link, is that of the *Designated Router*, or DR. In the DR scheme, each Area either elects for itself one DR and one Backup DR for redundance, or the DR and BDR are configured manually on non-broadcast link types. The DR functions as the authoritative source of updates to the link state databases of the routers in its Area, receiving all Link State Updates, performing the SPF calculations and then using LSAs to all the routers in the Area as well as border routers in other Areas to propagate the new link state. The link state database is updated and distributed as normal. All "internal" routers in the Area form adjacencies with the DR and the BDR, and its Backup DR, and only these, while other routers at Area borders will also maintain other adjacencies.

The Designated Router, therefore, is a concept removed from the router types (ABR, ASBR and so on) listed previously; a router being elected a DR does not specify exactly its connectivity to other routing domains/Areas, except that it must have a link instance connected to the Backbone Area.

The DRs in the AS form a Connected Dominating Set (CDS) for the entire AS, and each DR forms a single-vertex CDS inside its own area. Take note that this means that the CDS graph edges do not represent actual physical connectedness, or point-to-point network links, but rather adjacencies.

An important consequence of the DR system, is that on a broadcast network like Ethernet the traffic associated with exchanging routing information between routers is severely reduced: if every router were to build its own routing information and transmit to everyone else over broadcast, the amount of traffic associated would approach n^2, for n routers. Using DRs reduce this complexity to $2n$, as only the DR and BDR transmit routing information. Furthermore, it greatly reduces the processing and memory required for computing the LSDB. The implication of this is that the DR scheme allows OSPF networks to scale more easily, especially in conjunction with the Area scheme.

The Designated Router is elected according to a scheme which uses a configurable priority weighting, ranging between 0 and 255, which is contained in the OSPFv3 Hello packet headers that each router transmits. A weight of 0 implies that the router may not be a DR at all. Ties are settled by selecting the router that either has the highest router ID (a value determined either by the highest loopback ID on the router), or by the highest IP address amongst its interfaces. The second place router is selected as a backup DR.

Two noteworthy limitations of the DR scheme are firstly that it depends upon the network to be one which permits only bidirectional links, to ensure reliable link state update dissipation, secondly that it must be restricted to networks using a Broadcast Interface type on its routers.

2.5.6 Non-broadcast Multiple Access and Point-to-multipoint link type

NBMA links support more than two routers per link, unlike point-to-point, but lack the ability to broadcast packets. Examples of network link types that are supported by this link type are X.25 and ATM. Essentially, the link consists of circuits between each router.

The point-to-multipoint link type likewise does not have a broadcast capability, but unlike NBMA does not assume that all routers are one hop away. Originally this interface type was intended for 'cloud' subnetworks, like a Frame Relay network. Because of its connectivity limitations, P-MP interfaces do not elect a DR; instead, the Hello protocol is used for neighbour discovery only. All routers are adjacent to all others.

At the start of radio link networks being deployed, it was assumed that the P-MP interface type would be sufficient for accomodating the limitations in connectivity caused by the medium, such as line-of-sight or hidden nodes. However, in practice, the lack of broadcast implied that neighbor discovery and maintenance was exceedlingly costly as network sizes grew, consuming unacceptable levels of

resources from already constrained wireless links. Additionally, they lack a DR mechanism since DR election convergence cannot be guaranteed under such circumstances, increasing the number of adjacencies. These limitations are the main concerns adressed by the introduction of the OSPF-MANET wireless interface type, discussed in a separate section.

2.5.7 Flooding scopes in IPv6

Since IPv6 introduces new addressing semantics which permit a different kind of packet flooding, three new flooding scopes have been introduced for OSPFv3. These are the Link, Area, and Autonomous System flooding scopes. The first type will only flood packets within a single Link, and an LSA originated by a router will be resent on all Links the router is a member of; they are never forwarded beyond the Link.

The Area flooding scope will likewise keep packets within the Area on which they are emitted. Router LSAs will be flooded on the Area scope. The LSAs usually flooded with this scope serve to inform other routers about the address prefixes associated with the Link, and announce the link-local addresses of the router originating them. The link-local address of a router is only used to forward packets across one hop, and so they need not be flooded beyond the Link, since all routers on a Link can hear each other.

The AS flooding scope will flood LSAs to all routers in the Autonomous System across the Backbone Area. The common type of LSAs to be flooded with this scope are External LSAs.

2.5.8 Point-to-point Link type

The point-to-point link type is quite simply a PPP line or similar connecting only two hosts. All configuration is manual, and periodic HELLO messages assert that the link is working. These links are not included in any closer study in this thesis, as their security is guaranteed as long as the keying procedure and host integrity is secure. It is listed here merely for the sake of completeness.

2.5.9 Proposed OSPFv2 Wireless Link (Interface) type

An IETF Draft [1], last expired in November 2005, suggests adding a Link type (in OSPFv2 parlance, Interface type) which merits mention in this thesis, as it can be seen in conjunction with the later sections on the OSPF-MANET candidates. While not implemented as an RFC, the draft itself is well written and is well worthy of a read to familiarize those who are used to OSPFv2 semantics to the thoughts motivating OSPF-MANET.

As has been mentioned previously, the wireless interface type must be compatible with a network in which broadcasting is unreliable, either because

of line-of-sight, hidden nodes interfering or node mobility, and in which packets must be assumed to perhaps traverse several hops between hosts - unlike an infrastructure-based wireless networks, where the access point is always one hop away. The draft itself mentions that MANET networks are but a subset of the types of networks with the previously-mentioned properties.

The basic tenets of the proposed interface were as follows:

- Using multicast for reliable flooding
- No DR election
- No adjacency building

This required the addition of a new LSA type, the Link State Flood LSA, as well as introducing Multi-Point Relays, known from OLSR terminology, for flooding overhead reduction. Each routers MPR set would be announced using a Wireless Hello, which would include two-hop neighbour information. Compare this with the ordinary Hello messages of the existing OSPF link (interface) types, which only included one-hop neighbours. This information is used for MPR selection, as each node will keep selecting MPRs until all its two-hop neighbours are covered by at least one MPR. Since links are not necessarily bidirectional in a wireless link, only routers with which the host has a two-way link will be electable.

While database synchronization is carried out, it cannot be assumed to be identical, thereby putting the link (interface) type somewhat at odds with the classical definition of link-state routing, in which the entire network topology is common knowledge to all routers. This implies also that the adjacency concept is redundant on the wireless link type.

The wireless link type has not been introduced into OSPFv3. Instead, the OSPF-MANET working group is attempting to standardize an interface type which will fulfill the same functionality. A separate section is dedicated to these proposals, and these are the subject of the security discussion which concludes the thesis.

2.6 The OSPF process

The internal operation of an OSPF router is mainly subject to the dispositions of the software implementing it and the wishes of the vendor. Certain behavioral constraints are, naturally, specified by RFC2328/2740; others are configurable.

2.6.1 When to emit and expect packets

There are three main timers for an OSPF router to maintain. All timers must be equal in each router. There is no negotiation of timer periods in OSPF networks; it must be set manually by each administrator. This is a possible problem in a MANET setting, where autoconfiguration is a virtue and centralized administration is possibly unavailable. The main timer is the OSPF Packet Timer. As mentioned, it can be set to ten seconds by default, but a shorter interval will increase convergence ability in paralell with a rise in overhead.

2.7 How OSPF routers communicate

OSPFv3 uses five packet types for exchanging information between routers, all transmitted by encapsulation in IPv6 datagrams. The area type in which the packet originates and the packet type determines to where and in what manner it will be flooded. The main OSPF packet type for link state exchange is the Link State Update containing up to several Link State Advertisements, LSA. There are several types of LSA, each providing various types of link state according to the router type and Area they are sent from.

The LSA is the basic data structure through which link state is distributed in the AS between routers, and is also the manner in which the link state is stored in the Link State Database, synchronization of which between two routers implying adjecency, as has been mentioned.

An important divergence in LSA handling occured in the process of developing version 3: an LSA will now *not* be automatically discarded by a router if it has an unknown type code. Rather, the router can flood them as link-local (see the previous section of flooding), or alternately, it can be configured to flood the LSA in accordance with its flooding scope. While the router will forward the unknown LSA, it will not add it to its own SPF calculations. This development is intended to make OSPFv3 networks more accomodating to upgrades, as a subset of routers added that support some new feature implemented by a new LSA type can implement this functionality by continued reliance on the LSA being flooded in spite of not being understood by legacy systems in between.

2.7.1 The OSPFv3 Header

The header below, 24 bytes long, is common to all OSPF packets. A property of OSPF highly relevant to the routing security auditor is the absolute demand OSPF places on this header to be well-formed; if any of the fields are outside of the alloted range, the packet will immediately be discarded. The implications of this security-wise will be discussed further in the thesis. OSPF packets are, as mentioned, embedded directly in IP datagrams. The IP header should have TOS set to 0, specify protocol number 89, and preferrably set the Precedence field in

the IP header to INC (INternetwork Control) to allow OSPF traffic right-of-way to ordinary IP data.

The OSPFv3 header, differing from v2, notably includes no IP addresses. All identifiers are simply unique 32-bit integers, and do not follow IP address semantics.

2.7.2 Header Structure

<table>
<tr><td>01</td><td>03</td><td>05</td><td>07</td><td>09</td><td>11</td><td>13</td><td>15</td><td>17</td><td>19</td><td>21</td><td>23</td><td>25</td><td>27</td><td>29</td><td>31</td></tr>
<tr><td colspan="4">Version (0x03)</td><td colspan="4">Type (1-5)</td><td colspan="8">Length (Packet plus header)</td></tr>
<tr><td colspan="16">Router ID</td></tr>
<tr><td colspan="16">Area ID</td></tr>
<tr><td colspan="8">Checksum</td><td colspan="4">Instance ID</td><td colspan="4">Reserved (0x00)</td></tr>
<tr><td colspan="16">OSPF packet
...</td></tr>
</table>

Version is mandated to be set to 3 for all OSPFv3 packets, and length the entire length of the packet in bytes, as could be assumed. Both the Router ID and Area ID are 32-bit integers. The router may well be configured to only accept OSPF packets originating in a specific area, or to only accept those from designated router IDs, but both fields will initially not precipitate possible discardment at ingress.

The type field must be an integer from 1 to 5, or the packet is discarded. The types available are:

- Type 1 HELLO packet
- Type 2 Database Descriptor
- Type 3 Link State Request
- Type 4 Link State Update
- Type 5 Link State Ack

Each packet type is described in detail below.

2.7.3 The Header Checksum

Before progressing to the bits and bytes of the various packet types in OSPF, the checksum should be brought to our attention, as this thesis focuses on routing security, and checksums are commonly seen as a security feature. This checksum is the same type as defined for IPv6; the complement of the 16-bit ones complement sum of the packet. The basic algorithm is as follows:

1. Order the packet in words (2 bytes)
2. If the length of the packet is not a multiple of 16, pad with 0 at the end *quantum satis*
3. Set the Checksum field to 0
4. Add the two first words, with a carry from the HSB to the LSB
5. Proceed to add the resulting one's complement sum to the next word
6. Once all summation ends, complement the final sum

As we can plainly see, this checksum is not intended to be a cryptographic-strength checksum - in OSPFv2, this is handled by the variable-length Authentication field, and in OSPFv3 it is dispensed with entirely in favor of using IPSec. Rather, it is a continuation of the OSPFv2 practice of including a checksum to correct transmission errors. Nevertheless, the checksum adds a layer of complexity, or more correctly, a boundary on the form of OSPF packets to avoid them being discarded, which may have significance later when the forgery and modification of OSPF packets is discussed.

2.7.4 Type 1 - The HELLO packet

As mentioned, OSPF bases its operation on routers discovering neighboring routers, as well as maintaining contact with them periodically. This is accomplished using the *HELLO packet*. These packets are transmitted without forwarding at a default of ten second intervals on a broadcast interface. They consist of a normal OSPF packet header appended by a list of the DR and BDR, a list of routers from whom HELLO messages have been received, an interval specifying how long to wait between HELLO packets, options, and the priority (for DR election) of the router

An important implication of the HELLO protocol is that changes in the network topology may not be detected faster than the HELLO packet interval. If a router does not receive the expected HELLO packet from another router within a reasonable grace period, typically forty seconds, it will assume that router to be off-line, set the interface with that router do state "Down", and notify adjacent routers.

The HELLO emit interval is an important parameter of OSPF traffic overhead in a network, along with the size of the HELLO packets, which is fixed in OSPFv3.

2.7.5 Type 2 - Database Descriptor

A complete set of routing information is maintained internally in each router in a link state routing protocol. In OSPF, this information is organized as a database, the

link state database. Maintaining this database is a collective effort, as the database must be kept common to all routers to guarantee reliable routing.

As noted earlier in the document, router adjacency means that routers possess the same routing information, or link state, and that they will maintain a mutual relationship of exchanging updates to this information while the adjacency persists. In OSPFv3, all routers in an area are adjacent on multiaccess links *only* to their Designated and Backup Designated Routers. OSPFv3 distributes link state database information in the shape of DD (Database Descriptor) packets. These packets, when received, will give the arrived router a "directory listing" of the entire link state of the router with which it is forming an adjacency. This "listing" consists of Link State Advertisement headers (see below).

Database Descriptor packets, in short, arrive serially at the receiving host and are processed to allow it to obtain an overview of the Link State database by the Link State headers. Thereafter, once the DD synchronization is complete, Link State Advertisements will be filled in to complete the database according to their ID and sequence number. The new router itself requests the LSAs it deems it needs. Routers will also periodically request Link State Advertisements that have gone stale.

2.7.6 Type 3, 4 and 5: Link State Advertisements, Requests and Acknowledgements

OSPF packet type 4 is the LSU, the *Link State Update*. It is a packet consisting of an LSA header, with the appropriate type set, and one Link State Advertisement.

Link State Advertisements are, as mentioned, data units holding information about an active link between to routers, or even a whole subnetwork, as well as the identity of the originating router Through reliable flooding the router can make the assumption that all routers that need to obtain the LSA, eventually will, by retransmits through neighbouring routers. An important quality of LSA flooding is that a router may not change the content of an LSA it forwards on behalf of another router.

Each LSA has a header, separate from the OSPF LSU packet header, which includes the originating router ID, age, sequence number, and the LSA type. LSA type is provided in hex, giving the extent of how it is to be flooded in the network, see Figure 4.

Type 3 and 5, Link State Requests and Link State Acknowledgements, contain no link state of their own, but merely serve as control packets in the LSA exchange process. Requests are, in short, a listing of one or more Link State Advertisements, by ID, the requesting router requires. This can either be because it is missing in its LS database or because the current LSA has expired after one hour. Acknowledgements resemble Requests, but confirm receipt.

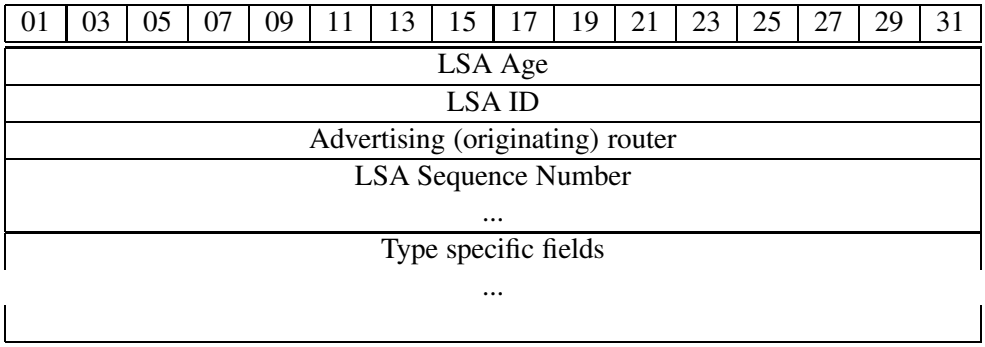

Figure 3: The Link State Advertisement Header

OSPFv3		OSPFv2	
LSA Type	Description	LSA Type	Description
0x2001	Router	1	Router LSA
0x2002	Network	2	Network
0x2003	Inter-Area Prefix	3	Network summary
0x2004	Inter-Area Router	4	ASBR Summary
0x4005	AS External	5	AS External
0x2006	Group membership	6	Group membership
0x2007	Type 7	7	NSSA External
0x008	Link	N/A	N/A
0x2009	Intra-Area Prefix	N/A	N/A

Figure 4: LSA types in OSPFv3 and OSPFv2

Link State Advertisements, to complicate the already somewhat crowded bestiary of OSPF packet types, are further subdivided into a number of specialized LSA types according to the type and location of the originating router. A comprehensive list of Link State Advertisement types is given below. Keep in mind that the LS*U* is distinct from the LS*A*: the latter is encompassed by and carried by the former, and the former contains no link state.

While Database Descriptors outlines the link state database, Link State Advertisements are the actual data structure in which link state is held. Link State Advertisements are identified by a number, address-based and determined by for instance the originating router or the network from which they arrive. A Link State Advertisement that arrives from outside the AS will have an ID that is the network mask of the originating network. Each LSA type has a different scheme for making these identity numbers. To differentiate between Link State Advertisements with similar ID, OSPF uses a Sequence Number to differentiate. This Sequence number is kept as a counter inside each router. It plays a crucial role in ensuring that only the most recent routing information is admitted into the Link State Database.

A Router LSA, shown in Figure 5, has the ID of the originating router, that

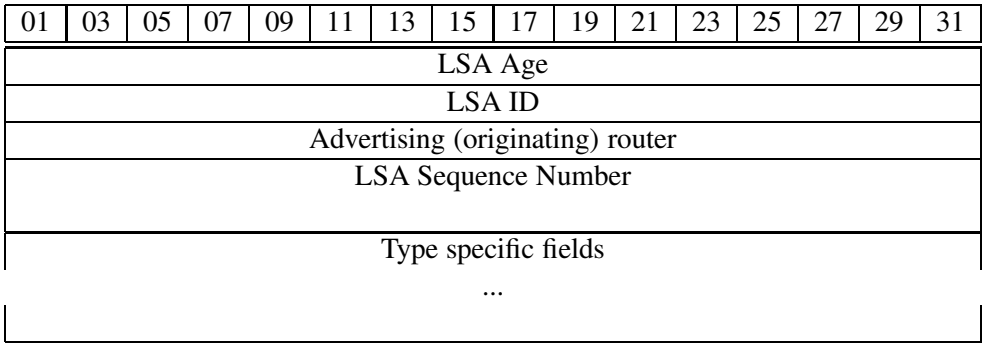

Figure 5: Router LSA

is, the router which sent it. Each router sends out a Router LSA for each area it belongs to, containing all links it maintains within that area - its set of active interfaces and neighbours. Using these, and reliable flooding, each router in the routing domain can learn the network topology of the OSPF routing domain. Most Link State Updates in a common multiaccess network will be of this type, and in an AS where all routers are connected by point-to-point links, the only one, in contrast to broadcast networks, where network LSAs will be aggregated by these and used instead by the Designated router.

Network LSAs contains information about each broadcast subnetwork, most importantly the routers. They are particular to broadcast networks, as they lose relevance on other non-broadcast interface types. The ID of a Network LSA is the IP address of the Designated Router. Following this is the advertiser ID,

The OSPF Area system is implemented by type 3-5. Type 3, the Inter-Area Prefix or Network Summary LSA, is generated by an ABR (Area border router). These advertisements are a means of distributing routing information from one area to another. They contain an addressing summary of the entire area using a netmask that can be used by other networks to infer what address ranges are represented by the area. These LSAs are the only link state that leaks between Areas. As a consequence of this, adminitrators may elect to hide prefix ranges from other Areas if so wished, for instance to create address ranges that are suitable for machines that require elevated security and should not be visible outside the Area.

Type 4 LSA

Type 5 LSA

Group membership LSAs are not relevant to this thesis. They describe the members of multicast groups in MOSPF (Multicast OSPF.)

2.7.7 Type 3 - Link State Request

A link state request is a simple packet type, which simply contains a list of LSA identifiers that the originating router doesn't have, or which have expired. In this

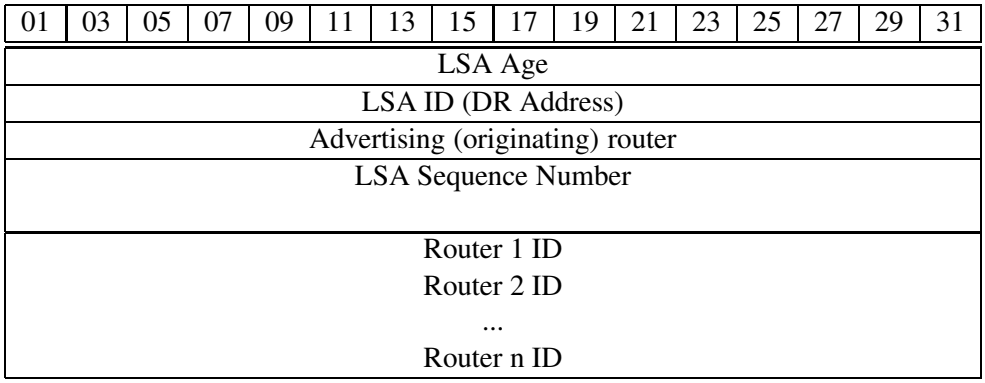

Figure 6: Type 3 Network LSA

respect they are almost excactly similar to the Link State ACK.

2.7.8 Type 4 - Link State Update

The Link state update packet contains an LSA, flooded to all routers adjacent to the DR, which has been altered by a change in link state. In itself, it is of little interest; it contains Link State Advertisements and is flooded where possible. The LSA

2.7.9 Type 5 - Link State Ack

To ensure reliable flooding of the LSAs across all interfaces, the DR will retransmit unacknowledged Link state advertisements. This retransmission is unicast to interfaces which have yet to acknowledge. The acknowledgment must specify the sequence numbers of the LSA packets. LSA acknowledgment may also take form of the recipient router returning it in its entirety, if it detects a newer version of the same LSA is already installed in the LSDB.

2.8 Commentary

OSPF is quite extensive, as has been demonstrated in this section. This is not a consequence of designer neglect - rather a logical consequence of OSPF being able to offer the fast convergence, link type versatility, loop-free high-quality routes and scalability that are its main selling points.

From a security perspective, a high degree of “intricacy” is usually not considered if not undesireable, then at least not something to strive for in itself. Implementing software like a routing daemon in a secure manner is complicated, because security auditing code for potential buffer overflow weaknesses or similar exploit entry points is costly and demands highly skilled programmers. However, it is likely in the case of routing protocols that the host security of the system on which the daemon is to run should be given at least equal attention, since any attacker with root access on a system can

3 Adding a MANET interface type to OSPF

A great number of articles and drafts have been authored over the last few years concerning the demands and contraints, as well as the design and implementation of, MANET routing protocols. Several protocols have been proposed, with two of the more successful having been made into formal RFC specifications by the IETF; OLSR in RFC3626 [9], and AODV in RFC3561 [37]. The former is a Link State routing protocol, developed from OSPF but substituting the DR mechanism with an entirely different Multipoint-Relay (MPR) scheme which creates a connected 2-hop graph of the MPR set, while the latter is a distance-vector protocol. Both have been extensively tested, and several implementations are available.

3.1 Motivations

OSPF has several proven advantages that makes it desirable to adapt an interface type for it that acknowledges the limitations of MANETs. It is, as mentioned previously, by now a mature, stable and well-known Internal Gateway Protocol, with a set of interface types (see above) which makes it versatile and adaptable to a wide number of currently used network types. There is no inherent property of the basic link state aggregation and generation scheme of OSPF that forbids it from being able to operate as a MANET routing protocol.

In a broadcast network, the DR method of distributing link state without undue overhead, makes OSPF routers converge quickly and efficiently. Open standards available for router developers to implement. The sum of all these factors, and more yet, is that OSPFv3 today is the dominating IGP on the market. They also make the prospect of using it to route traffic in MANETS enticing. The main reason for this, is that OSPF in an extended, wireless form would be easy to integrate into an existing OSPF network, as the former envelops the latter. Furthermore, the strengths that OSPF exhibits in a common multiaccess broadcast-enabled network may well extend into the realm of MANETs with adaptation: scalability and overhead reduction.

3.2 Main challenges

Two important problems must be alleviated in a MANET OSPF interface type. Firstly, flooding of messages must be made reliable in spite of the medium limitations of non-guaranteed connectivity. Secondly, convergence must be made to occur faster to accomodate the mobility of the nodes, although without increasing message overhead to the extent that it suffocates the constrained medium. The interface type must have some kind of Designated Router scheme, which may become possible once reliable flooding is provided, because simply assuming the non-broadcast ability of the Point-to-multipoint interface type will lead to a prohibitively large amount of adjacencies.

3.2.1 Adaptation to topology changes

Wireline networks enjoy the benefit of being relatively static. Mobility, when it occurs, is usually discrete, in the form of micromobility (a node changing its position within the AS). Routers are generally immobile within the topology, and are also usually designated and specialized for the task. If a router is moved, it happens as a planned down-time event. Once it is regains connection to the routing domain, the neighbor discovery and database synchronization mechanisms ensure that Link state is built anew. Ensuing LSA updates announce the new router. If the router needed to move, and change its neighbors, not discretely but continuously, these mechanisms would correspondingly need to be respond in turn, primarily by decreasing the intervals between Hello packets, reducing the lifetime of LSAs. This, however, when implemented, results in often unacceptable overhead: the majority of packets transmitted over the constrained wireless medium might become Hello and LSA packets. This is demonstrated clearly in [21].

3.2.2 Connectivity and the Designated Router

When OSPF works across Link types where this mechanism is available, the Designated Router maintains adjacency with all routers in the Area, making the DR and backup DR "linchpins", of the entire system. Even if a one-level "hot-swap" redundancy exists if the DR is lost, in the shape of the BDR, should both be lost in short time the consequence would be that routing stagnates while a new pair is elected. If this happens often, the network will suffer greatly as LSAs go stale in the non-DR routers. This is not a likely scenario in a well-planned wireline network - the prudent network administrator will configure and position his DRs in such a manner so as to minimize the Single-point-of-failure likelyhood, perhaps even going to the length of separating them both in terms of physical location and separate sections of the power grid. However, losing both DR and BDR within a short period of time is very much a possible, if not expected, event, in a wireless link and especially a MANET. Wireless transmission conditions can change rapidly with router movement in the shape of interference, line-of-sight and hidden and exposed nodes. Two-way links can neither be assumed because of the latter problems. How can we ensure that each router in a wireless MANET will always have a two-way link to its adjacent DR or BDR?

The point-to-multipoint Link type can fit the non-guaranteed bidirectional broadcasting of a wireless link, as mentioned in Section 2.5.8, detailing the proposed OSPFv2 Wireless interface type. While it has not been included in the official OSPFv2 specification, the thesis introduction mentions other proposals from the OSPF-MANET WG exist for a Link (interface) type extension to OSPFv3 which address the same issue. These extension proposals will be presented and compared in the following sections. The three of them are respectively called Mobile Designated Router, Overlapping Relays, and Multi-point Relays.

3.3 Two main proposals - Mobile Designated Router, and Overlapping Relays

There are numerous proposals to these problems, but two proposed protocol extensions of OSPF that address these problems have been selected by the IETF OSPF working group as the most viable alternatives. They are outlined and discussed in the following chapter.

3.4 Mobile Designated Router (MDR)

This proposed OSPFv3 MANET interface extension is specified in the Draft [34]. Advantages of the protocol are available in a Draft [35]. It is also documented further in [21] and in [44]. For the remainder of the thesis it will be reffered to as OSPF-MDR or MDR. While MDR not only describes the protocol extension proposal, it also can refer to a role that can be held by a router with such a Link (interface) active - where applicable the necessary context will be provided to eliminate ambiguity between the two. In [44] a fully functional simulator implementation for JSim is available for further study, should that simulation platform be desired.

3.4.1 Overview

The OSPF-MDR proposal suggests adding an interface for OSPFv3 in which the DR scheme of the Broadcast interface type adds resilience by allowing for more than one DR on each link, the set of which is always connected. The DR is under OSPF-MDR referred to as a Mobile DR, MDR, with the Backup DR being the Backup Mobile DR, BMDR. Flooding is optimized by restricting flooding to only (B) MDR routers, and is made reliable by flooding LSAs through adjacencies. While several DRs exist on the link, each router hails to one DR/BMDR pair only, effectively partitioning the network between DR/BMDRs, to allow for better scaling. Since LSAs are flooded across adjacencies, adjacency reduction is important for performance. Any router on the link will always either be on the CDS or one hop away from a node in the CDS.

OSPF-MDR differs from OSPF in that Hello packets include two-hop neighbour information, similar to the OSPF Wireless interface proposal. This information is used by the router to determine with which DR/BMDR it is to become adjacent, constructing a Connected Dominating Set (see figure) on the network.

To an Area outside of the MANET link, possibly containing non-OSPF-MDR capable routers, the Area will be advertised as a Point-to-Multipoint link, in spite of the broadcast capability.

3.4.2 Modifications to the Hello protocol

Differential Hellos allow for overhead reduction. To increase protocol agility, Hello messages are transmitted every two seconds. By differential Hellos is meant that the packets only document changes from the previous packet. This provides a substantial reduction on protocol traffic on the interface. To allow new nodes to quickly learn the two-hop neighbor status of its neighboring nodes, every third Hello packet is a full packet. These intervals are configurable if a higher degree of reactivity is desirable.

3.4.3 The MANET Designated Router

Instead of dispensing with the DR scheme of OSPF and replacing it with an OLSR-similar AOR set, OSPF-MDR allows for a mobile, general DR, elected in a similar manner to that of OSPF, but with the provision that an existing MDR is preferred, to reduce overhead associated with synchronization of the Link State database whenever a new MDR is elected.

The MDRs are selected in such a manner that they and the adjacencies between them, forms a Connected Dominating Set that spans the entire network. This CDS is referred to as the *adjacency subgraph*. The adjacency subgraph thereby forms a "backbone" for the link, reducing overhead while ensuring reliability in flooding.

Each node may form either one or several adjacencies with MDRs, referred to as its *parent*, making the adjacency subgraph connected or bi-connected. By being bi-connected, the adjacency subgraph may not be made disconnected by breaking of one single vertex, making for a stronger and more resilient backbone.

The election procedure, as in the broadcast DR scheme, is according to the configuration of the router, but combined with information about the two-hop neighbourhood it senses through the Hello packets.

3.4.4 MDR election

Each node determines whether it should be an MDR. The information it bases its decision upon, is a comparison for all its neighbors of the set of each router defined as (MDR Level, Router priority, Router ID). A note should be made on the description of this procedure in [34], as the ordering method it uses is that of *lexicographic ordering*. In short, lexicographic ordering in set theory implies that given a set (x, y) and a similar set (x', y'), then (x, y) > (x', y') if and only if either x > x', or x >= x' and y >= y'. This implies that if a router has the highest MDR level of its known neighbors, it will set itself to be the MDR of that group, whereas if another node has an equal MDR level, then the tie will be settled by comparing the router priority, and finally the router ID if the tie persists. This is in all respects similar to the DR election in ordinary OSPF.

There are three MDR levels; 2, 1 and 0 - respectively indicating the status of MDR, Backup MDR, and MDR Other. The latter is the general node, which selects parents from the (backup) MDR set, and does not forward LSA packets on the incoming interface. This flooding procedure avoids excess flooding.

3.4.5 Flooding

As LSAs are only sent across adjacencies, the MDRs carry out the forwarding. When an LSA arrives on an OSPF-MDR interface, the router will immediately retransmit the LSA across the same interface. Backup MDRs will only flood after it has been determined that a neighbour exists that is not covered by a retransmit.

3.5 Wireless OSPF - Overlapping Relays (OR)

WOSPF-OR is described in detail in the Draft [8]. It extends OSPF with several important concepts. An implementation in the shape of a Quagga patch has been completed as of 2006 [22]. It is also documented in [21].

3.5.1 Incremental Hello protocol

The simplest and easiest extension simply consists of reducing the Hello packet interval markedly, leading to a much faster response to topology changes. However, this would also naturally imply an increased overhead in an already resource-constrained network. To alleviate this, WOSPF-OR redefines the Hello protocol to only include the changed nodes, either absent or newly added, to the Hello packet neighbor list. It does not compensate for the increased frequency, but the reduction in overhead is important.

3.5.2 Link Local Signalling

To provide for the extra signalling information required for MANET operation, LLS has been proposed as an extension of existing OSPF packet formats, with the proposed data format being the TLV - Type/Length/Value blocks, appended or “piggy-backed” onto existing OSPF packets. The TLV block is rather simple, consisting only of a type identifier, the length of the block, and the associated values. Several TLVs may be appended onto one packet. The LLS system is completely transparent to legacy OSPF packet protocols, a point of central importance to the transparent interoperation of WOSPF-OR and OSPFv3.

3.5.3 Overlapping Relays in detail

The specific problem of operating wth Designated Routers on wireless broadcast or point-to-multipoint interfaces is adressed by the Overlapping Relay scheme. In short, Link State updates are flooded reliably and efficiently by means of each router selecting a subset of its neighbors to transmit LSAs, the *Active Overlapping*

Relay (AOR) set. This scheme resembles strongly the MPR set of OLSR, and the purpose of both is similar: to reliably flood LSAs while reducing the redundant transmissions as close to the possible minimum. OLSR itself enjoys RFC status from the IETF [9].

The AOR set is built in voluntary nodes. To flag willingness, each router includes two TLV blocks, both appended to Hello messages. The Willingness TLV sets the node's willingness to serve in the AOR set, represented as a value between 0 and 255, with 128 as the default. The AOR TLV simply sets one of two bits, called the 'A' and 'N' bits, respectively meaning Active and Non-active. Non-active nodes will not be required to transmit LSAs for their selector, but may be called upon to do this if all else fails. This distinction permits low-resource nodes to be spared the processor overhead and battery drainage that constant retransmissions incur.

Upon determining its AOR set, the node X will first construct a set of all its neighbors willing to serve as AORs. For each node Y in the candidate AOR set, X calculates their degree D(y). The degree of an AOR candidate node is the amount of one-hop neighbors it has, minus the nodes in the candidate set and X. It compares the neighbors of each node Y, and adds those that provide the only known route to a neighboring node unreachable from X to the AOR set, proceeding until all neighbors of nodes in Y have been covered. Finally it prunes the AOR set by removing as many of the nodes with the lowest willingness while preserving connectivity. For the OLSR initiate, this scheme may seem similar to the MPR selection algorithm, and it is. Indeed, one recent WOSPF-OR implementation (Holter-WOSPF-OR) reuses the source code from a well-known OLSR implementation for simplicity.

3.5.4 The Non-active Overlay Relay set

Upon reception of an LSA, the router will make a series of tests, each determining if and when the LSA is to be retransmitted. Firstly, if the router is a part of the AOR set, it will retransmit immediately. If it is a non-active overlapping relay, it will still retransmit if no retransmission has been detected within a standoff period. This ensures reliable flooding even if every node in the AOR set fails. This feature is where WOSPF-OR departs from OLSR, as the latter provides no "backup" MPR mechanism, but is crippled if all the nodes in the MPR selector set is disabled.

Essentially, the Non-active OR set is the rest of the nodes not selected to the AOR, along with those routers that have set the AOR-TLV 'N' bit. It is worth noting that retransmission is compulsory for all nodes if necessary. This adds another degree of reliability to the flooding scheme, along with the ordinary LSA acknowledgements of OSPF.

3.6 MPR-OSPF

Another proposal bases itself on the MPR (Multi-Point Relay) mechanism of OLSR. It is documented in Draft [3]. Along with its dispensal of the Designated Router mechanism altogether, for reasons stated below, it also extends OSPF at a very fundemental level by adding an OSPF Interface Type specifically tailor-made for wireless ad-hoc networks, named the Wireless Interface Type. The Draft is recently revised, with a working implementation being currently tested for performance [35].

3.6.1 MPR Wireless Interface Type

The MPR Wireless Link (interface) type defines an interface where broadcasting should be thought of as "half-complete". That is, only a subset of the routers neighbors can be assumed to receive the broadcast transmission. This is a close approximation of real-life transmission conditions in the wireless medium. To permit adjacency reduction on this interface type, a new kind of flooding scheme is needed that dispenses with the OSPF method of selecting a DR and Backup DR. This Link type is similar to the OSPFv2 Wireless Link (Interface) type proposal described in Section 2.5.8, as well as in a separate Draft [1].

3.6.2 Adjacency management in MPR-OSPF

Two role types exist in an MPR-OSPF network. Similarly to OLSR, these are MPRs and MPR Selectors. The MPR and its selectors are adjacent to each other, leading to a high number of adjacencies. A node can, and will usually, assume both roles; a node is an MPR or an MPR Selector in relation to one other node.

3.6.3 MPR selection

The MPRs are selected similarly to the MPR selection of OLSR and the OR selection of WOSPF-OR; each node iterates through its neighbor list and selects MPRs that cover unique two-hop paths, until all two-hop neighbors are covered, after which the MPR set is again pruned to remove redundancies. Each MPR is notified by its MPR selectors that it has been chosen. This is a radical difference from ordinary OSPF, where each router *by itself* decides whether to become a DR/BDR, on account of the Hello protocol; the router is elected - not selected.

3.7 Comparison of the proposals

Some amount of debate in the IETF MANET Working group has ensued on the virtues and faults of the three above proposals. Most of the key issues revolve around the below topics. Overlapping Relays and Mobile Designated Routers are, by virtue of their longer history and greater level of progress in terms of simulator and working implementations, considered widely to be the more viable contenders

for the interface. OR and MDR were compared extensively in [21] in 2005, with MDR being recommended for further development as it both demonstrates a lower degree of overhead by reducing adjacencies compared with a robust convergence. Both have been demonstrated to show a remarkable reduction in overhead compared to the existing point-to-multipoint interface, while still offering strong forwarding and convergence performance. However, scaling is still an issue, as neither proposal manages to approach $O(n^2)$ complexity; that is, the overhead scales faster than the square of the nodes, as could be hoped for.

While both protocols are comparable in terms of adjacency reduction, it was consistently found in [46] that MDR provided increasingly optimal routes than OR.

3.7.1 Adjacency management

There is a great deal of concern in the research community as to how adjacencies in routing protocols in MANET settings may be minimized, for obvious reasons: the fewer redundant adjacencies, the fewer redundant LSA floodings and consequently improved network capacity. According to [35], OSPF-MDR has a distinct advantage over OR in how it reduces these adjacencies.

3.7.2 Performance

Both OR and MDR have been implemented, and have seen extensive testing in simulation. In the Draft [35] it is shown by simulation how in the setting of a dense network of 100 nodes within a 500 meter wide square grid, and transmission range of 250 meters, OR will generate 4 times as many adjacencies as MDR. This is, if repeatable under test-bed conditions, certainly a major improvement in overhead reduction. However, criticism of the simulation-only results obtained has been forthcoming, pointing out that simulations are regarded as good indicators of the protocol functioning correctly, but poor tools for measuring real-world performance. The reasoning for this is that simulations, while perfectly executing the state machines of the routing protocols, omit concerns of performance actors which are hard or impossible to properly simulate. These include human-generated radio noise compromising frame transmission, variations in vendor equipment in terms of buffer sizes, coding or even protocol implementation, chaotic traffic patterns and realistic mobility models.

This is likely to remain a central point of contention, as the protocol that can boast the better performance will be regarded favourably when selecting a standard for a routing protocol for use in the resource-constrained world of MANETs.

3.8 How OSPF-MANET proposals differ from existing OSPFv3 Link types

The new Link (interface) type will not, as has been stated, completely redesign the OSPFv3 protocol as it is documented now. The basic operating principles it abides

Change	MDR	OR
SPF calculation	Yes, but within standard	No
LSA types	Yes	No
Extend OSPF header	No	Yes

Figure 7: MDR and OR changes to OSPFv3

by - Link State routing, LS database, Shortest-Path First route calculations, Area hierarchy - remain pillars.

MDR dispenses with the Network Summary LSA, as it has no meaning in a MANET, instead substituting it with an extension of the Router LSA which describes its immediate neighbors, to a variable degree: at the strictest configuration, the MDR Router LSA only includes the neighbouring routers to which the originator has a full adjacency.

OR, on the other hand, suggests adding a new TLV (Type, Length, Value) block to the OSPFv3 header, indicated using LLS (Link Local Signalling) in the header to signify that extensions are present. These extensions may be ignored by non-OR routers, providing backwards compatibility. These extensions to the header are used for the particular signalling used by OR routers. The OSPFv3 LSA catalogue is kept intact without additions, and are used to forward Link state on the MANET interface.

Under MDR, the Shortest Path First algorithm is somewhat altered, in that it, to quote [34],

> "allows any routable neighbor to be a next hop to a destination. We note, however, that RFC 2328 [authors note: OSPFv2 standard, see [31]] also allows a non-adjacent neighbor to be a next hop, if both routers are fully adjacent to the DR of a broadcast network. Allowing any routable neighbor to be a next hop is a generalization of this condition to multihop wireless networks."

As such, MDR does place a constraint on the internal state of the OSPF router, but not in a manner which puts it directly at odds with its standards specification. This would likely be a benefit to vendors reluctant to completely rework complicated implementation details.

Differential Hello signalling is a common feature of all. OR uses Link Local Signalling to indicate if a neighbor has been dropped from the neighbor list.

3.9 Concluding remarks on OSPF-MANET

Currently, MDR and OR seem set to remain the top contenders for the standardized proposed by the MANET Working group. There is some discussion on whether one or two standards should be proposed; opponents of this option point out that the

charter of the WG is to create one proposal, and that the lack of a general protocol interface extension that can function in all MANET scenarios is also contrary to the intentions behind creating the WG. This thesis chooses to direct its efforts towards the OSPF-MDR proposal.

MDR has been shown in [21] to provide more optimal routes than OR in a variety of simulation scenarios, while at the same time having decent overhead reduction by keeping adjacencies at a minimum.

4 Security services, IPSec and wireless network security

“Security” is a word with a large number of connotations, but for which many definitions may apply. Some attention should be afforded to define what is meant by such terms as *computer security*, *network security*, *routing security*, and indeed, security as a whole.

4.1 Cryptographic security services

Security services are in short those mechanisms which any system can offer to prevent, detect and recover from attacks. When the assets to be protected are *information*, or part of an information infrastructure, the security services are mainly provided by cryptographic means.

The IETF provides an Internet Security Glossary, which offers generally accepted definitions of the specific security services in terms of which goal each is intended to achieve. In addition, the IEEE X.800 specification offers a more specific classification of services. However, for reasons of the extended use of RFCs which this thesis supports itself on, using an IETF publication for these definitions is probably the better, if more general in nature.

The following definitions are all provided by RFC4949 [45]. While Digital signatures and Non-repudiation are often grouped as security services, they will be treated separately.

- Data confidentiality

  > "The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]." (...) ISDs SHOULD NOT use this term as a synonym for "privacy", which is a different concept.

- Data integrity

  > (I) The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. (See: data integrity service.)
  >
  > (O) "The property that information has not been modified or destroyed in an unauthorized manner." [I7498 Part 2]
  >
  > (C) Deals with constancy of and confidence in data values, not with the information that the values represent (see: correctness integrity) or the trustworthiness of the source of the values (see: source integrity).

- Authentication

> (I) The process of verifying an identity claimed by or for a system entity. (See: authenticate, authentication exchange, authentication information, credential, data origin authentication, peer entity authentication.)
> (C) An authentication process consists of two steps:
> 1. Identification step: Presenting an identifier to the security system. (Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service.)
> 2. Verification step: Presenting or generating authentication information that corroborates the binding between the entity and the identifier. (See: verification.)
> (C) See: ("relationship between data integrity service and authentication services" under) data integrity service.

The foremost security services relevant to routing protocols are data integrity and authentication. Without the former, no LSA can be trusted not to have been altered in transit. Without the latter, the assuredness that the authenticated router is in possession of a secret key - a weak form of identity.

Data confidentiality is likely more relevant to the domain of User data security [20].

Another often-referenced security service is *availability*, or the ability to resist Denial-of-Service attacks. This security service is somewhat particular compared to integrity, confidentiality and the like. The reason is that it isn't really produced by cryptographic algorithms, but by management, planning, provisioning and, most importantly, by the other security services: if all data transmitted in a session is intentionally corrupted, leading to checksum failures and subsequent packet drops, then that session is lacking availability. That session then must employ integrity and perhaps also authentication to return availability to itself. Availability, then, is not analogous to *authorization*, which is the more precise security service of regulating access to a system, denying anyone who is not permitted such access and permitting anyone who is allowed. A system can include a multi-user operating system, or the system itself is a physical lock such as a code lock on a door.

Several *security protocols* implement one or several of these security services. The main security protocol operating on the network IP layer is IPSec. Other notable security protocols are 802.11i, offering link layer confidentiality and other services for the IEEE 802.11 wireless network standard, and TLS, operating at the transport (TCP) layer.

4.2 Definitions

The word 'security' comes from Latin *securitas*, 'that which assures something', 'guarantee', or even *tranquilitas animi* - 'peace of mind'. We could extend

this definition, then, to define security as, “that which assures us that unwanted events do not occur”. This is one of its classical definitions. It certainly does encompass our desired routing protocol behaviour. But the question remains if we are better served by a stricter definition. The connotations that the word ’security’ itself have with most computer scientists are connected to illegitimate, illegal or malevolent activities and intentions. So, by narrowing our definition, and adding the provision of security being a continuous effort against ever new threats and attacks, security could be said to be “that which acts against malevolent activities occuring”. We now have a more useful starting point that excludes the myriad of ways in which computer systems can be subjected to unwanted (such as Byzantine) events. *Securing* something means to modify it in such a manner that it may be called *secure*, or having the property of *security*.

There are, as mentioned in the introduction, three main security disciplines which this thesis concerns itself with, aside from the umbrella term of Information Security. These are host, network and routing security. The two latter are intimately connected, but there are also strong connections between host and routing security. These are not explored in-depth in this thesis, but consider the prospect of a rootkit offering an attacker full, undetectable control of a central network router in a very large and important network of strategic importance.

- Computer (Host) security - The discipline of securing a computer system, both its hardware component and the software it executes.
- Network security - The discipline of securing a computer network, both the hardware and software of its dedicated nodes, across all end-to-end network protocol layers, thereby protecting the integrity and confidentiality of the data transmitted over the network itself and assuring network operation and the availability of services the network provides. End-to-end implies that the protocol layer interacts with a correspondent across a link.
- Routing security - The subdiscipline of network security that seeks to permit the routing services of the network to operate securely.

4.2.1 A note on User data security

User data security is centered on the end user, the receiver of the services provided by the host and the networks it is connected to. It does not imply that system administrators have confidence in their users never doing unwanted things. Rather, user security borrows from other security disciplines: computer (host) security offers local protection of application memory space and files on disks, for instance, while network security offers confidentiality of user data during transmission, authorization (user access control), authentication and digital signatures. In an 802.11 wireless network, user security can be assisted by link-layer encryption protocols like 802.11i implemented as for instance WPA supported by key handling

by the TKIP protocol, and by network access control (NAC) mechanisms like 802.11x or PacketFence. In short, user security focuses on protection of user data first and foremost.

The confidentiality and integrity of user data is not critical to routing protocol operation. It is therefore important to distinguish between routing data and user data, as the difference in their security requirements is reflected in the cost in terms of memory, computational resources, and network overhead that must be comitted to meet them. Under any circumstance, the wireless networks seen as the typical application of an OSPF-MANET interface usually have good confidentiality services implemented at the link level, notably 802.11, which offers strong cryptographical protection of link layer frames using the WPA protocol, especially with TKIP keying activated. When keying is unavailable, higher-layer services such as IPSec or TLS at the transport layer should be employed.

In spite of this, it should be noted that routing information confidentiality in certain applications becomes a concern [32] [23]. The foremost example of this would be in a military tactical setting where an enemy is able to eavesdrop on routing information in a tactical network. As all who have some knowledge of military intelligence is aware of, the main method by which intelligence is produced is by aggregation of minor, non-critical pieces of information into a whole which adds up to provide more information than the sum of its individual components. Routing state could very well provide such a source of information: notably, establishing the identity of a highly adjacent router in a link state network can serve as a strong indication that the router is located at a Command and Control site, or, alternatively in the case of a Distance Vector algorithm, repeated Route Requests for a specific host could pinpoint it as a potential HQ site worthy of closer scrutiny. Willingness to be elected an MDR on an OSPF-MDR link can, when set to a very low value, possibly be perceived as an indication of a radio site which expects to see a large amount of mobility, or which has a low battery capacity or a low-gain antenna. The presence of these assumptions together could be interpreted to coincide with, for instance, a node carried by a reconnaissance patrol if its Hello messages have a higher than normal rate of changes in their MDR field. In such a way, a routing protocol whose state is not protected to offer confidentiality can act as an information leakage for the benefit of enemy intelligence efforts.

4.3 IPSec

The purpose of the IPSec security architecture is to provide the security services of authentication, confidentiality, integrity control and non-repudiation, replay protection and some amount of confidentiality to traffic flows to IPv4 and IPv6, the network layer of the TCP/IP protocol stack. The main advantage gained by this approach, rather than making security an application or transport level issue, is the transparency provided to the application layers, avoiding costly and difficult re-implementation. In addition, IPSec defines cryptographic keying protocols.

IPSec was first described in RFCs 1825-1829 in 1995, and was subject to a complete redesign in 1998 with RFC2401-2412, which nonetheless retains the basic concepts of the first. A third update came with RFC4301 through 4309. The last update does little more than provide an additional keying mechanism. The first generation is mutually incompatible with second and third.

Two modes of operation are defined for IPSec; *Transport* and *Tunnel*. The distinction is that while Transport mode IPSec is encompassed by the IP header, as only the payload is subject to full protection, Tunnel mode encapsulates the entire IP packet. Their respective uses generally consist of end-to-end communication between hosts, and secure tunneling between two separated trusted domain, across an untrusted domain. The latter is generally put to use in the shape of VPN - Virtual Private Networks.

As a protocol suite, IPSec defines two protocols for packet security, Encapsulating Security Payload and Authentication (ESP and AH). Their differences lie in what security services they offer, and to what extent they encompass the protected packet when run in transport or tunnel mode. Authentication Header is intended to function as a protocol for offering authentication and integrity, while ESP is intended to offer confidentiality. Numerous suggestions have been made that AH is itself encompassed by ESP running a Null-Encryption scheme, and as such is redundant. Counterarguments that payload inspection is at best risky using Null encryption have been made, but the two protocols nevertheless continue to co-exist.

4.3.1 How IPSec works

IPSec relies on the concept of the Security Association, SA, between two nodes. A traffic flow in one direction using one security service uses one SA. This implies that an IPSec session involving two nodes desiring authentication and integrity need to create four SAs. The SA itself consists of a cryptographics key, an identifier of the cryptographic algorithm to be used, and any parameters for the algorithm. The details of IPSec SA negotiation are usually best left with the protocol specifications. The important part to notice is that the negotiation of an SA can *only* occur between two hosts, and that it cannot be duplicated. In other words, if hosts A and B negotiate SAab, it is impossible for host C to negotiate an SA called SAac or SAbc which is equivalent to and interchangeable with SAab.

IPSec offers automated, dynamic key management. More on this is provided in the next section.

What services IPSec is to offer to which packets is detailed in the Security Policy Database (SPD), which specifies whether an incoming or outgoing IP packet should be protected, discarded or bypass IPSec entirely. In the case of the SPD stating that the packet is to be protected, the SPD must also provide the protocol, mode, algorithm and appropriate parameters necessary, or provide a link to a corresponding entry in the Security Association Database (SAD). The

Nr.	Src	Dst	Protocol	Action
1	any	any	SNMP	discard
2	any	any	TCP	bypass

Figure 8: A small SPD

SAD consists of Security Associations, which again are constructed of a 32-bit unique identifier, a 64-bit (32-bit optional) sequence counter for replay protection in conjunction with a parameter determining the size of the sliding window, and identifiers for which algorithms to use. Figure 4.3.1 shows a very small example SPD.

4.3.2 IPSec cryptographic algorithms

The cryptographic algorithms available to IPSec are outlined in RFC4901. Those that are mandated or recommended ("MUST" and "SHOULD", as defined by RFC2119) are 3DES (TripleDES) and AES-128 for encryption, SHA1 for integrity checking and authentication, and Diffie-Hellmann Group 2 (1024) and Group 14 (2048) for key exchange.

3DES and AES are both block ciphers standardized by the NIST. They cand both be considered to be computationally secure at the time of writing. The former algorithm remains computationally secure in spite of efforts in recent years that have led to successfull cryptanalysis of the DES algorithm by collective efforts. The keyed hash algorithm SHA-1 has in recent years been subject to strong, non-partial, non-limited cryptanalysis efforts. One of these in 2005 reduced the complexity of finding a collision from 2^{80} to 2^{69} [51]. It was improved the same year to 2^63 by the same group that achieved the previous result. Further attacks were made the following year [7] by another research team. As a result of this, the

NIST has announced that it intends to replace SHA-1 with the stronger SHA-2 by 2010. A short discussion on hash function attacks follows in the next section.

4.3.3 Cryptanalysis of hash functions

The authentication algorithms mandated by IPSec are SHA-1, AES-HMAC and MD5. SHA-1 is mandated, while AES is, again, strongly recommended. MD5 is optional, but recent years have seen strong cryptanalytic attacks on this algorithm. This includes *preimage attacks*, in which a forged plaintext m_{forged} can be chosen by the attacker for a plaintext $m_{authentic}$ such that

$$H(m_{forged}) = H(m_{authentic})$$

The second preimage attack is vastly more critical for routing security than *collision attacks*. A hash collision is the phenomenon that a random message m_{random} exists for any message $m_{authentic}$ such that

$H(m_{random}) = H(m_{authentic})$

The main reason for the criticality of pre-image attacks for routing protocols, is their conservatism in accepting packets: only those who conform exactly to the standardized norm are normally accepted. Randomized payloads generated with a collision attacks will be discarded at ingress long before they can exert any damage. A preimage payload conforming to the protocol, however, represents a potentially viable threat. However, the fact that the crafted payload also needs to pass the stringent validation efforts of the routing protocol adds another layer of protection.

4.3.4 IPSec key management

Key management in IPSec is essentially a synonym for SA negotiation. It is therefore of central importance to how well IPSec works: the cryptographic algorithms are only as robust as the mechanisms used to distribute their keys are. The purpose of key management goes beyond merely putting the same key securely in each host: negotiation of a number of parameters and similar state is likewise carried out through this process. Handling it manually generally scales poorly - an SA is a one-way, one-service provider, and as the amount of SAs rises quickly, so does the amount of work that is needed for manual key management. IPSec specifies two dynamic key management protocols: IKE(v1), documented in RFC4901, and IKEv2 in RFC4306. Both use features of protocols like ISAKMP, Oakley and SKEME, and use public key cryptography based on the Diffie-Hellman exchange to establish a secure channel across which to negotiate parameters and exchange keys. IKEv2 is a much simplified IKE(v1); while the first version has no less than eight different methods to establish the state, with various (dis)advantages, IKEv2 only has one, four-message exchange. IKEv2 also benefits from a much stronger protection against DoS attacks than IKE, in that it actually seeks to affirm as strongly as possible that the corresponding host exists before beginning CPU and memory-expensive cryptographic calculations. The lack of such affirmation in IKE has proved to be a powerful DoS exploit.

The default KM protocol specified by RFC4301 is IKEv2 [25]. IKEv2 is far from as complex as IKEv1 [39] [28] [18], and still relies on a Diffie-Hellman exchange for establishing a secure channel across which to distribute key information, in whichever form it may have been generated. This DH exchange forms the first keyset which is then used further by the two hosts of the SA. A primitive example of a DH exchange can be found in Figure 9. Real-world values of a and b will at least be 512 bits, and preferrably at least 1024 bits long.

Part A and part B first agree to a prime number p and a base g, the prime is the modulo of which all calculations will be carried out. Each generates an integer a and b in secret. A sends B $g^a mod p$, while B sends A $g^b mod p$. A then calculates $(g^a mod p)^b mod p$ and vice versa. Since $g^{ab} = g^{ba}$, both parties will have established the same key. Finding a or b will require to solve the *Diffie-Hellman*

Step	A	Message	B
1		<- $p = 23, g = 5$ ->	
2	$a = 6$		$b = 15$
3		$5^6 mod 23 = 8$->	
4		<- $5^{15} mod 23 = 19$	
5	$K =$		$K =$
	$(19^6 mod 23 =$		$(8^{15} mod 23 =$
	2		2

Figure 9: Diffie-Hellman key exchange

01	03	05	07	09	11	13	15	17	19	21	23	25	27	29	31
IPv6 Header															
(Hop-by-Hop, Routing, Fragment IPv6 Extension Headers)															
Next header				Payload length				Reserved							
Security Parameters Index															
Sequence number															
Authentication data - variable according to algorithm, multiple of 4 bytes															
(Destination options extension header)															
TCP/UDP															
Payload - variable length															

Figure 10: IPSec Authentication Header in Transport mode

problem: given g^a and g^b, what is g^{ab}? This is closely related to the Discrete Logarithm problem: given $g^x \equiv amodn$, for an n that is the size of a cyclic group, what is the x that gives a its value? Algorithms exist which reduce the complexity of finding x, but none approach polynomial time. A more thorough discussion of the subject is found in [47].

4.3.5 Authentication Header

The authentication header is documented in RFC4302 [26]. Under IPv6, the AH will be located directly below the IPv6 header in the shape of an Extension Header, if applicable behind the Hop-by-Hop, Routing (not to be confused with OSPF!) and Fragment Extension Headers. AH will be announced with procotol number 51 in the preceding header. AH protects certain elements of the IPv6 header, notably those that are immutable. The latter excludes ToS and Time-to-Live and other minor fields which are meant to be altered in-transit.

The cryptographic services provided by AH are Data integrity and Authentication (see [45]).

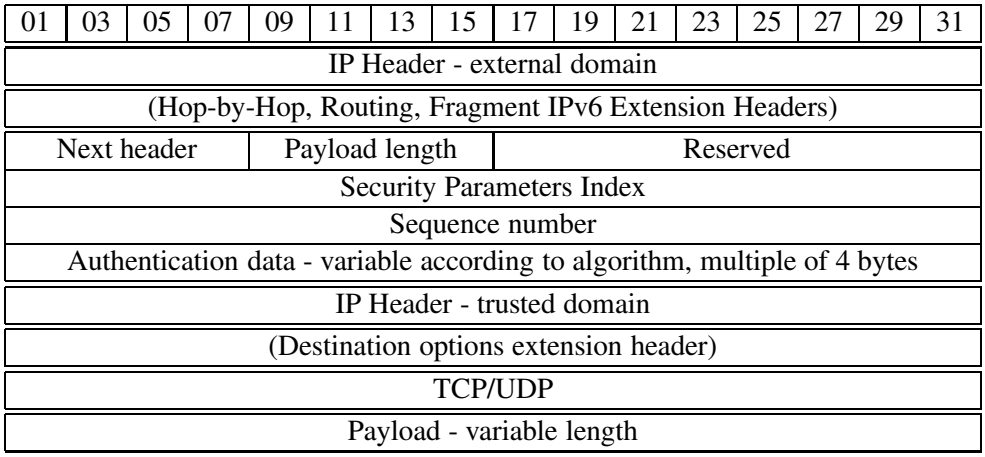

Figure 11: IPSec Authentication Header in Tunnel mode

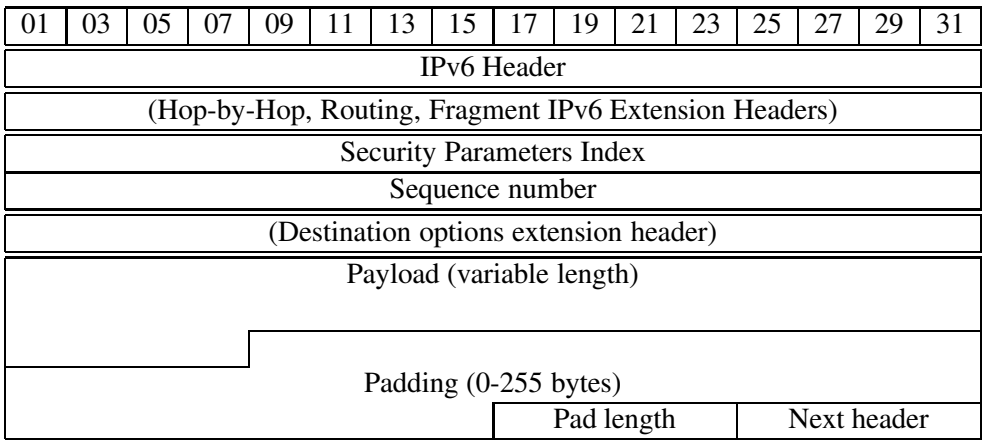

Figure 12: IPSec Encapsulating Security Payload in Transport mode

4.3.6 Encapsulating Security Payload

ESP, protocol number 50 in IPv6, offers the services of Authentication, Integrity and Confidentiality [45]. It is defined in RFC4303 [27]. A sequence number scheme offers protection agains replay attacks. These are attacks in which an intercepted packet is re-transmited by an opponent for some gain.

ESP uses two algorithms for confidentiality; 3DES and AES, both in Cipher-Block Chaining mode, the latter also available in Counter mode. Only 3DES is mandated, but in recognition of its advanced age and the advantages of a more software-oriented algorithm, AES-CBC is strongly recommended, as is AES-CTR. In addition, a NULL algorithm is electable for when confidentiality is not needed.

ESP does not, unlike AH, protect the IP header.

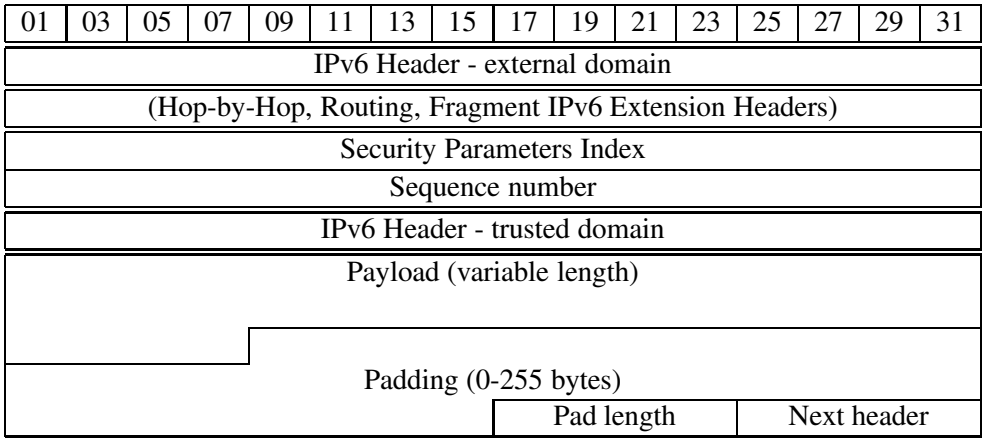

Figure 13: IPSec Encapsulating Security Payload in Tunnel mode

4.4 Wireless network security

Focusing on the MANET as the "Wireless network" depicted here, we see a number of crucial security issues. Network security aims to offer security services to network links, protecting user data, ensuring service availability and providing non-data oriented security services like authorization and digital signatures. This task certainly becomes harder in a MANET [53], where the wireless link type and the lack of central monitoring and infrastructure as well as physical exposure and absence of a certification authority add to the arsenal of the attacker, while doing little to that of the defender [29]. The lack of a clearly defined border for the network, in the same sense as a network socket or the plastic jacket of an Ethernet cable to in a wireline network, demands multiple "lines of defense" [52], not meant to be encased within each other as "ablative armour" meant to be burnt off slowly, but each addressing one or a subset of security issues to create solid, gap-free security. Still, there exist security strong points of MANETs. These include its very distributed nature, eliminating central Single-points-of-failure [20].

Wireless network security is often thought to revolve around link-layer security, notably 802.11i protocols such as WPA and TKIP, as well as the issues of physical layer availability through resistance to signal distortion (jamming).

4.5 Routing security: resilience, fault-tolerance or robustness?

Routing security is commonly seen as a cross-layer problem, in spite of the routing protocol operating inside or in conjunction with the network layer. As has been mentioned in the introduction, host security and network security are the two crucial security disciplines in this regard, with routing security concerning itself with auditing and improving the security of the processes which constitute the routing protocol - identifying, assessing and counteracting what [24] refers to as "General vulnerabilities".

Operating system, or host, security, would concern itself with preventing usurpation, and maintaining accountability, confidentiality, and authentication inside the router, in particular while contemporary routers, even minor consumer models, increasingly take the form a highly specialized server running a multi-tasking, multi-user OS [50]. Network security adds to routing security by providing the services of non-repudiation, confidentiality, authentication, resource availability et al. to the packets transmitted across the link containing user data and routing information.

What is *achieved* by routing security? One good summary could be that the security of a routing protocol is that quality it has which permits it to operate with adequate performance. Performance of a routing protocol can be, as has been mentioned, be a product of convergence speed, the quality of routes, and the amount of overhead, as well as other qualities deemed desirable, such as battery conservation. These qualities should be assured in a secure routing protocll in spite of deliberate, malicious attacks against its functioning, which is essentially establishing and maintaining relationships with other routers, across which to exchange relevant and correct information permitting routing tables to be built.

For a routing protocol to be called *resilient* or *fault-tolerant* or *robust*, it should be capable of adequately handling its designated tasks in spite of unforeseen events occurring to routers, nodes or links. The distinction, then, between routing and network security becomes difficult to ascertain, as the two are intermingled. One important difference is that user information security is generally omitted from the scope of routing security: while the routers themselves need end-to-end security among themselves for routing information exchange, the protocol in itself does not offer this service to the ordinary packets routed by means of it, instead deferring such services to another process or another protocol layer altogether.

The security service primarily employed by routing protocols is authentication/integrity. The common mode of operation is to embed keyed hashes made with a common key inside the routing packets; a fresh digest is then computed on each payload upon reception and compared. The verification that the local and remote hashes are equal implies that the payload is legitimate: firstly, no unauthorized host lacking the key could have created it, nor can it have been modified in-transit. Naturally, the key use implies some moderate amount of authenticity of the identity of the host who used it. Looking it at what it accomplishes, the more natural term to use for this security service is integrity, since this is exactly what it is intended to protect, but authentication seems to have become the commonplace term, albeit slightly erroneously, since originator authenticity is only secondary and less-than optimal using this method.

Judging from the secure routing protocols which have been proposed and papers on the subject of routing security, confidentiality seems to be given a secondary priority to authentication/integrity in routing protocols [6] [50]. The

likely cause of this is the fact that most of the routing information can be deduced by means other than payload inspection: HELLO messages, for instance, are broadcast across the medium; a reasonably knowledgeable attacker with access to the medium can listen freely for packets using for instance protol 89 (OSPF) using a simple packet sniffer, then parse the payloads and construct a reasonable network topology. This insight is reflected in the fact that only NULL encryption is mandated in ESP mode for OSPFv3 as documented in RFC4552 [15].

4.6 MANET routing security

A number of secure MANET routing protocols have been proposed [6].

The MANET, being a relatively recent network model, has been under security scrutiny from its inception, because of is features of structure and composition: any node can enter and leave at will, and being a multi-hop environment in which dedicated routing infrastructure is not assumed, every node should be able to when needed to participate in the routing process, or indeed any other service needed for the MANET to offer the desired level of services to the nodes.

There have been efforts into MANET routing security. Without securing routing protocols, MANET performance can suffer from attacks as routes decline in quality more rapidly because of mobility and the difficult link conditions.

Most security challenges faced by wireless networks are also applicable to MANETs, some to a potentially far greater degree. These include the ease of eavesdropping and physical signal jamming, as well as the physical exposure of nodes to a hostile environment, such as a battlefield or surroundings that are not encompassed by any physical security measures. Another important point is that of resource availability - without ready access to power, nodes are limited to battery power, and attacks such as mentioned previously can be devised to prevent their operation by causing undue power drainage.

The unregulated network membership assumed by this thesis compounds these problems, as an attacker often with ease can enter a malicious node into the link.

4.6.1 Dynamic Key Management in MANETs

In order to function as intended, cryptographic security services need strong keys which can accomodate their proven weaknesses. MANETs need such security services because of their more exposed nature, as described in [29] [52] and notably by Zhou and Haas in 1999 [53].

In particular, IPSec as mandated by RFC4552 needs keys which accomodate the known security weaknesses of MD5, since this is the weakest cipher available to AH/ESP when operating in accordance with the RFC [15]. Since key distribution in the wireless medium is vulnerable to eavesdropping, and since nodes in a MANET should be able to join at will for the duration of the network, including “late-entry

nodes", secure and dynamic key distribution is required. There are a number of works concerned with this problem, notably [20] and [13].

4.6.2 Security strong points of MANETs

As described in [20], one strong security point of MANETs is indeed its distributed, generalized nature: dispensing with access points and other forms of dedicated infrastructure removes the possibility of network failure due to centralized single points-of-failure.

4.6.3 Modes and protocols

While it may seem apparent from IPSec design that routers, including those operating under OSPFv3, *must* employ Tunnel mode, this is circumvented by the fact that OSPF traffic is always local to the AS, with clearly defined borders to other networks. At these borders, ingress filtering drops IP frames with protocol type set to 89. In this local perspective, routers become hosts to one another, permitting the use of transport mode. Tunnel mode nevertheless remains optional, but will only provide additional security for OSPF compared to Transport if there are fields in the IP header which are security critical to OSPF. AH and ESP differ further in whether they offer payload confidentiality. It should be noted that from the perspective of IPSec, OSPF packets constitute the payload - it does not distinguish some particular segment designated for "user data"; anything found behind the IP header is per definition IPSec payload.

It should be noted that there is general agreement that the non-protected IPv6 header under ESP opens up the possibility of a limited replay attack on OSPF [4] [24] that could cause disruptions in adjacencies, and RFC4552 further states that manual keying cannot counteract such a replay attack.

5 Security in OSPF version 2 and 3

Research literature abounds with proposed attacks against routing protocols, including the big three: OSPF, IEGRP and BGP [4]. The extent to which these have been implemented in practice varies, but for the major part, they remain theoretical or confined to test beds. One consequence of this is that routing protocol attacks have been downplayed in favour of more immediate or easily executed attacks, such as transport-layer based DoS-attacks or SNMP weaknesses. The more recent creation of accessible tools to perform such attacks has returned attention to routing security and routing attacks. Even still, while DNS has suffered several malicious attacks, few such case studies have appeared on OSPF or even routing protocols in general, including the notoriously insecure RIP.

5.1 The IETF and routing protocol security

The design process of early routing protocols like RIP rarely if ever paid much attention to the aspect of security, presumedly not for reasons of negligence on the side of the designers, but rather as a consequence of the practical realities of the time: network users were overwhelmingly composed of scientists and professionals, whom by virtue of professionalism and idealism would not be assumed to be willing to subvert or sabotage.

As has been mentioned, later years have seen an increase in the attention being paid to routing security research. The IETF has itself assigned a Working Group, named RPSEC, to the field, with a charter of determining both the generic security threats that routing protocols are exposed to, as well as establishing a documented set of security requirements that can be used by future protocol designers. Notable publications from the WG are in particular [4], “Generic threats to routing protocols”, a non-protocol specific attempt at establishing from where, by whom and with what routing protocol security can be menaced. It is exhaustive, including a section on potential adversary motivations (routing malfunction with the intent of sabotage or benefit in the form of financial gain) and capabilities (medium access, host security subversion). While the RFC is, as mentioned, non-protocol specific, it limits its scope consciously to that of well-known, implemented protocols, omitting the vast field that is experimental or suggested protocols, many of whom are developed specifically to address issues connected to routing protocol secority (SAODV, ARIADNE). While it documents techniques usable by an adversary in a routing protocol attack such as packet sniffing and falsification, it does not itself offer any practical insight into how this might be carried out. A separate section in this thesis addresses this, by demonstrating some well-known and universally available tools in use by both network administrators as well as the illicit hacking community to enact attacks.

5.2 Threat model

By *threat model* is meant the circumstances and constraints both attacker and defender are governed by. Adversary motivations can also be added to the threat model where needed for completeness.

One common threat model is the Dolev-Yao [12] model, which offers the attacker the benefit of being able to spoof both recipient and origin addresses of packets, as well as retrieve, modify, and re-transmit (replay) messages, but prohibits him sufficient cryptanalytical means to break cryptographic keys. In essence, under a DY thread model, well-keyed authentication/integrity mechanisms can defeat adversary attempts at spoofing and modification of packets. The term "sufficient" in terms of cryptanalysis capacity is a somewhat variable quantity: while cryptanalyzing an algorithm protecting a message whose contents are valuable can be wortwhile to the adversary even in the face of weeks of heavy computation, a routing protocol adversary is limited in his time scope by the relevance of the routing message as well as such replay mechanisms as may exist preventing admission of packets not within some timestamp or sequence number constraint.

Threat models also need to consider the physical protection of nodes, and their host security level, with the option of usurped nodes under the hidden control of the attacker taking part in the MANET or the routing process. We can refer to such usurped nodes as *Byzantine* nodes, as their behaviour is consistent with the definition of such nodes.

We should consider the means by which the attacker gains access to the target. In this case, our target is the MANET whose routing processes we are attempting to safeguard, hence the attacker will have gained access to the target when a node controlled by the attacker is within transmission range of at least one node in the MANET. OSPF packets are intended for AS-only scope, hence an OSPF boundary router will not admit packets set to protocol type 89 into the AS. This, however, does not imply that the AS is watertight against external routing information, potentially harmful, from entering into the system: an ASBR can, of course, still accumulate and dissipate routing information from other protocols into the AS, in particular from BGP.

Network security, as an end-to-end guarantor of the integrity and authenticity e.a. of packets, plays an important part in routing protocol security. Relevant to this thesis in particular is, of course, IPSec, a network security protocol suite offering a flexible set of tools that can be used for these purposes. The main alleged drawback of IPSec in a wireless network remains performance, both in terms of packet overhead as well as CPU and memory constraints in nodes. To establish the security level of OSPF in a wireless network, attention must be paid to this issue.

The Byzantine node is one such attack 'vector', the other is that of an external attacker moving into the network.

5.2.1 Byzantine nodes

On October 27, 1980, a network outage in the ARPANET of several hours occurred. Following recovery, an investigation into the event revealed it to be caused by an exotic hardware fault in one router: the routing message sequence number of one peculiar update had been modified by bit dropping, and because of weaknesses in the detection of bit errors in messages in routers, was transmitted in three exact copies, but with differing sequence numbers. This resulted in a network-wide loop in which these three packets were constantly retransmitted and queued internally in each router, resulting in routers going down due to processing and memory constraints. The event and its resulting rectifications in router design is discussed further in [40]. It sparked interest into the subject of designing routing protocols which could detect and recover from unforeseen events of a random nature, coined Byzantine events in [38]. According to the latter, a Byzantine failure is "caused by nodes or links which continue to operate, but incorrectly." Furthermore, "A node with a Byzantine failure may corrupt messages, forge messages, delay messages, or send conflicting messages to different nodes." This is contrasted with *simple* failures, in which the node or link ceases to operate at all. [38] is widely recognized today as a breaking point in the study of robustness, and thereby security, of routing protocols, after which this became a topic of concern during the design process. It introduced design criteria for routing protocol robustness that were disregarded previously: robustness had to exist in spite of different router vendors (standards compliance), and had to allow for non-centralized network management, notably.

Following the publication of [38], computer security experts began to examine closer the potential for malicious, Byzantine attacks on routing protocols. A seminal work in this regard was [5], in which notably the RIP protocol, at the time the leading IGP, was analyzed from a security viewpoint. This identified the concept of the man-in-the-middle packet modification by means of sending bogus routing information, diverting traffic through the usurped node for higher-layer processing and retransmission.

Figure 14 illustrates how a Byzantine node fits in a routing domain. The blue delineation describes the limits of the AS, and the blue arrows show adjacencies between routers across various links. One router has been subverted by an attacker, and an illicit (red) channel exists between the attacker and the usurped node. Through this illicit channel, the damager can inject information of a harmful nature into the AS through the adjacencies the Byzantine router shares with its peers.

5.2.2 External nodes

An external node attack is comitted by a node entering into the network. The node has access to the medium and can listen to link layer communication. It can under IPv6 participate in link-local network traffic without the need of stateful address autoconfiguration. The nodes already in the network participating in the routing

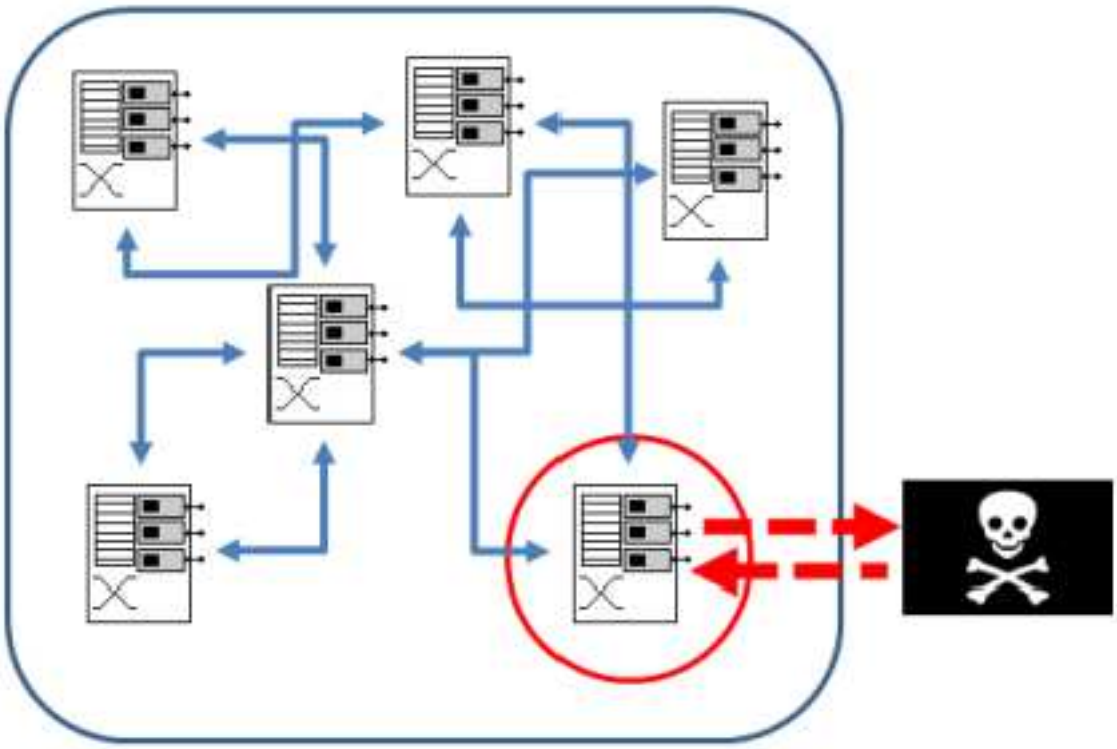

Figure 14: A Byzantine router in an Autonomous System

process may have been configured with keys manually, or there may have been some other keying procedure.

Figure 15 depicts a MANET routing domain in which some nodes are in movement, and where adjacencies are established. The attacker simply moves his node into radio range, and unlike the Byzantine scenario there is no need for an illicit, hidden data channel between attacker and node.

This thesis directs its efforts towards MANET routing protocols working in a threat model where any node can enter the MANET transmission range and join the network, but in which Byzantine nodes are not assumed. Nodes are moving in an open terrain, and are exposed physically. Why the need for a distinction? The reason is mainly that Byzantine node problems heavily involve host security, as an usurped node and a malfunctioning node both are in a sense indistinguishable for the network if the malfunctioning node begins to exhibit harmful behaviour. This means that the scope of the thesis would have to be extended into the host security of routers. Secondly, the external node attack vector becomes far more likely in a MANET setting, since the attacker gains a lower threshold for network admittance.

5.3 Active and passive attacks

An *Active* attack is one where the attacker provides information as part of the attack, actively interfering with the system. A *Passive* attack conversely implies that the attacker in a non-interfering manner eavesdrops for information. The passive attack can constitute the entire attack in itself, such as an attack on confidentiality, or as a preparation for an active attack. A more specific introduction to some potential active and passive attacks follows here, while a more detailed review can be found in [16].

5.4 Attacks on routing protocols

This section provides a quick overview of the most commonly referenced hypothecized and practically implemented attack types on routing protocols, notably in [50] [24] [49] [4] [36]. Not all are equally relevant to this thesis - the aim here is to focus on external attacks. In addition the thesis aims to limit itself to those attacks which target the operation of the routing protocol itself. This leaves attacks and explout that can only be or are best countered by network and host security outside of the scope of this thesis. This notably includes attacks that alter the IPv6 header or disrupts IPv6 functioning [33] or which mandate a subverted or faulty router (Byzantine node) [40] [38].

5.4.1 Denial-of-Service

Denial-of-Service (DoS) is *not* one specific attack, as most who know the term superficially associate it with HTTP-request flooding might assume, but rather a

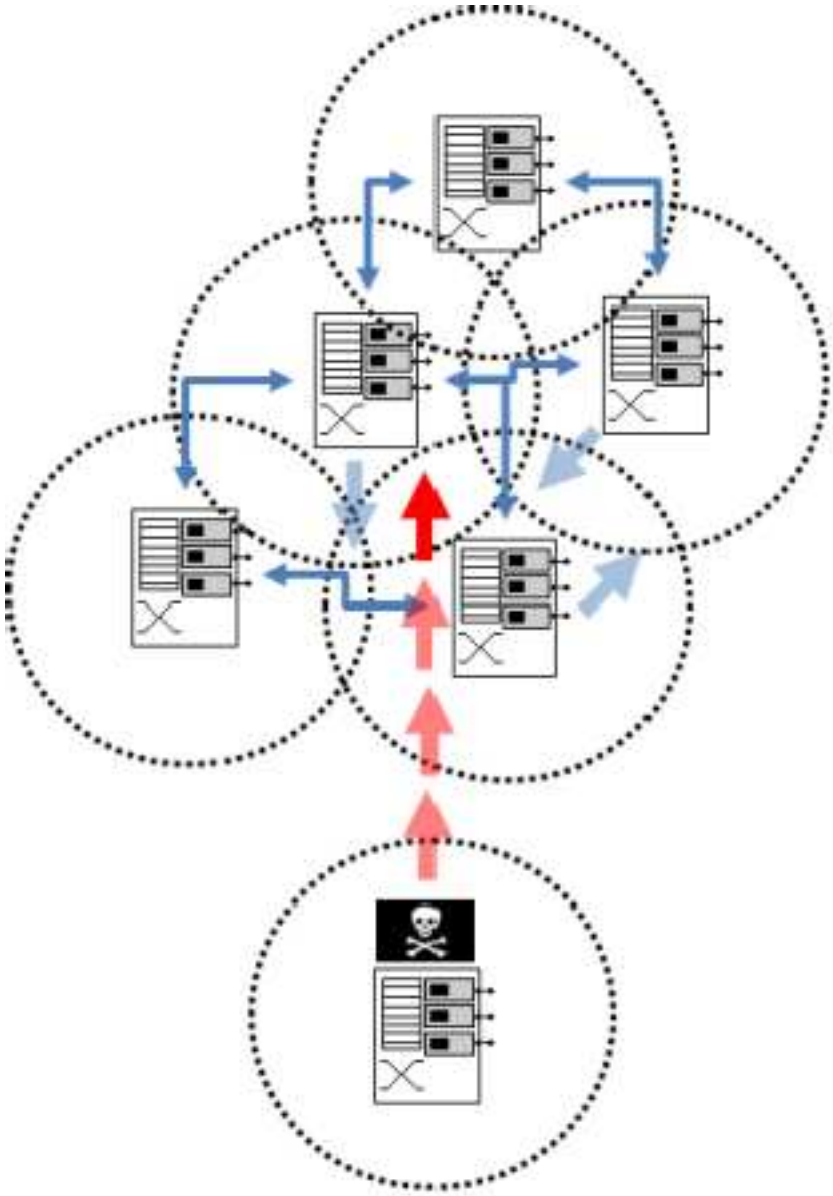

Figure 15: External attack into a routing domain

consequence of numerous attacks. The purpose of a DoS attack is, of course, to block or limit the access of a node to some crucial network service.

Can DoS be considered an attack type at all? In one sense, no, as DoS could be thought of as merely a symptom of an underlying "disease" - in this case a willed attack. However, by regarding availability as a security service on par with integrity, confidentiality and authentication, DoS in itself can be seen as an attack type.

5.4.2 Injection of erroneous routing information

An active attack in which the attacking node joins the routing process of the MANET and seeks to limit its functioning by means of injecting erroneous routing information, potentially creating the loss of or deficiency of existing network routes. The attack resembles the act of willfully turning road signs to create detours in a road network. This attacks forms the basis of black hole/gray hole attacks. The exact extent of the damage this attack can inflict is a function of the amonut of detours a packet needs to take due to the false routing information as compared to the optimized, shortest-path first route that would have otherwise been used, as well as the time the routing system uses to correct the erroneous route.

5.4.3 Injection of packets damaging the routing process

The actively attacking node once again joins the routing process and injects a "malformed" packet into the network, but this time, the packet employs weaknesses in the routing protocol in order to attack either the collective routing process or the specific routing process of one or more nodes. A highly effective attack against OSPFv2 has been demonstrated by Vetter, Vang and Wu in [48], where the injection into an OSPFv2 Area of a Linke State Update packet containing an artificially high Sequence Number in its header caused a testbed network to lose routing services for times approaching one hour. It would be natural to assume that this attack can also be performed under OSPFv3, as the sequence number still exists and has the same limitations. If so, one question is how the increased control traffic, and thereby faster sequence number rollover, will affect the damage caused by this attack.

5.4.4 Artificial redirection - black and grey holes

The actively attacking node takes part in the routing process, choosing at the attackers discretion one or several nodes for which the attacking node advertises falsely optimal routing metrics to other nodes, leading to the other nodes more willingly using the attacking node for multihop routes to the attacked nodes. Once routing to the attacked node or nodes is 'monopolized', the attacking node is free to either drop all packets destined to attacked nodes (black hole) or selectively remove certain packets, either at random or according to the attackers intentions

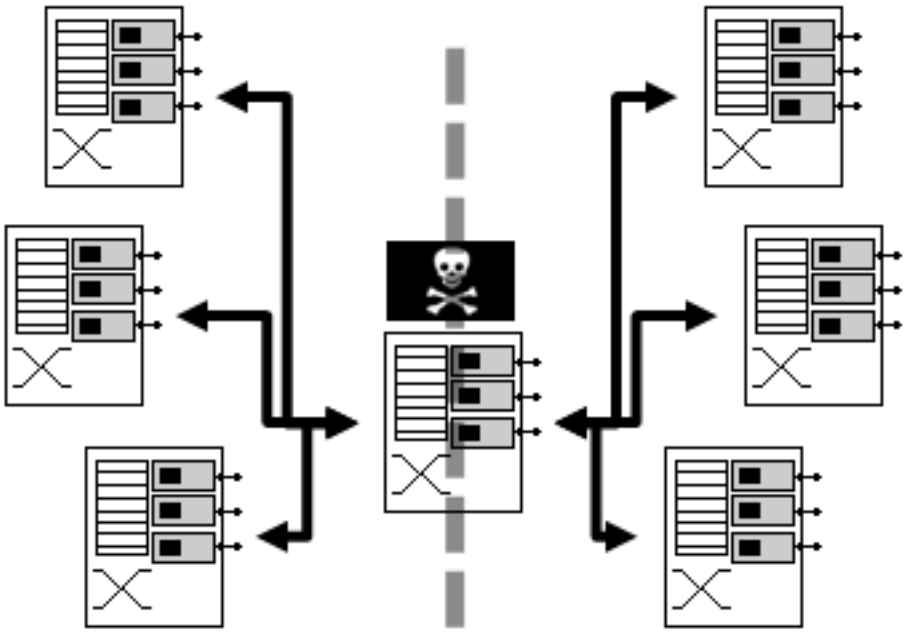

Figure 16: Network fragmentation attack

(gray hole). This attack type is particularly suited to *reactive* MANET routing protocols [36], including AODV. It could also be considered a Denial-of-Service attack.

5.4.5 Network fragmentation

By positioning himself in the route graph in such a manner that no path exists in the graph between the subgraphs A and B, the attacker will enjoy full control of all traffic between nodes in A and B. It is illustrated in Figure 16.

If the network has a homogenous traffic pattern, the attacker node will have the possibility to drop or otherwise tamper with approximately half the packets transmitted. Note that the attacker in the illustration is not a hub in a wheel structure, with the other routers as spokes: these still can route traffic amongst themselves without passing through the attacker.

The fragmentation need not concern routes only, but simply adjacencies. In this manner the attack will not be seen through a route visualization tool, but the attacker can hamper convergence capabilities.

As we can see in the figure, the attacker node forms a virtual barrier in the network which he may use to drop or selectively drop packets (see above on black and grey holes). Another opportunity is to consciously lower forwarding efficiency.

Executing such an attack needs to take into close account the way the attacked

routing protocol converges. An attacker seeking to partition an AODV network needs to offer consistently better routes from one side of the partition to the other, in order both to attain and keep the partition in place. It is far harder to execute in a link state routing domain, simply because the attacker has no influence over what other routers announce through LSAs. Therefore, to attempt something akin to a similar effect in a MANET setting where an LS protocol is running, the attacker would rather need to move his node into a favourable position, hoping to use range limitations to his advantage. In practice, this would likely be very difficult if not impossible. It is likely that this attack type, therefore, is of little danger to OSPF within each Area. Between Areas, OSPF works in a DV-like fashion, as mentioned in Section 1.4. The attacker, if in possession of an Area Border Router, could forge Network Summary LSAs in order to partition the Backbone. No reports of any attempt at such an attack have been encountered.

5.4.6 Geographical tracing

The attacker has a substantial intelligence resource, and has detailed information of the physical nodes, including properties like transmission strength and power. Using this knowledge in conjunction with routing information from an adjacent Link State Database, as well as physical-layer signals intelligence efforts, the attacker is able to make educated guesses with varying levels of precision as to the physical location of nodes. This attack model is mainly relevant to military battlefield scenarios. To counteract this attack the owner of the network needs to provide confidentiality to all routing messages, as well as possibly establishing a virtual network of encrypted tunnels between nodes to provide data stream confidentiality. The extent of this attack is largely a function of the opponent, hence it will not be a central attack to this thesis.

5.4.7 Power drainage

This attack 'type' resembles DoS in that it by itself isn't really a specific attack as it is a result of one. The attacker seeks to deny nodes operation by means of inducing them artificially to waste power at a faste rate. This could be implemented as a Network fragmentization attack. Perhaps as an analogy to Denial-of-Service, such attacks could be dubbed "Denial-of-Operation" (DoO). Power drainage attacks are mainly considered to be effective against sensor networks, because of the assumed small size of the nodes and their short battery life.

5.5 The OSPF Area mechanism under attack

OSPF offers the administrator the option of partitioning the AS into a series of discrete Areas, of which the central is the Backbone Area, Area 0. The remaining Area types are handled earlier in this thesis.

An attacker wishing to leverage the Area mechanism for an OSPF attack, is to consider the crucial importance of the Backbone Area. While subverting a Stubby Area with for instance a Maximum Sequence attack will render that Area useless for the duration, repeating the same attack inside Area 0 will not only affect the routers in that Area, but will also provide an effect that prevents efficient routing of routing information between Areas. In this respect, Area 0 becomes a Single-point-of-failure.

5.6 OSPFv2 Authentication

As RIP failed to scale to increasing network sizes, its replacements - notably OSPF - would often be designed with increased concern for robustness and security. This was not always the case, though, and security of routing protocols often was implemented by principle of "bolt-on" rather than "bottom-up". As directly stated in [48],

> A well known fact about many routing protocol designs is that they only consider simple failures, while security is usually an afterthought."

The possibility of malicious Byzantine nodes or of external malicious nodes entering the routing process are not usually completely left out of the design process considerations. OSPF, for instance, did consider such possibilities in that authentication was added. More background material about the creation of OSPF can found in [30]. While OSPF authentication is generally considered inadequate today, it still was much better than the complete openness of RIP.

OSPFv2 has been subjected to extensive security and robustness scrutiny, in accordance with its wide adoption compared to other IGPs. The IETF maintains a Draft [24] which describes those OSPF security vulnerabilities that are known and which could be used to disrupt the routing process, classifying them as follows:

- General - vulnerabilities resulting from basic properties of the network and the routing domain
- Protocol-specific - connected to the actual protocol mechanism, including OSPF message header modification
- Resource consumption - exhausting the resources of the router to deny their services to users
- Other protocols - vulnerabilities that arise through interaction with other protocols, like IP, and other routing protocols, like BGP

In addition, [50] highlights the OSPFv2 properties of *information independence and hiding*. The authors conclude that OSPFv2 is highly robust, and even provides some measure of built-in security, and three notable OSPFv2 security strengths are highlighted: information least dependency, the hierarchy of the AS partitions, and the strong mechanisms OSPFv2 uses to validate a packet upon ingress before it is accepted - excluding IP packet scrutiny.

The Draft shows that the security vulnerabilities of OSPFv2 mainly center around the lack of real authentication and packet integrity without using IPSec, due to the weak cryptographic authentication in OSPFv2, as well as the danger of the malicious, authenticated node. The latter can [50] with moderate difficulty launch a man-in-the-middle attack on an AS by using ICMP routing and router redirect control messages to announce a malicious node as a shortcut between two other nodes.

5.7 OSPF Fightback

Fightback is the postulated ability of OSPF to correct erroneous by means of each router immediately correcting any LSA received which purports to have been sent out from the router. This effect is merely a documented part of the OSPF protocol; any router receiving an LSA it sees itself as owner of, will check if it is containing information at odds with that of its own LSA database. If that is the case, the protocol assumes the LSA is outdated or damaged in some manner, and that the router as the data originator is responsible for rectifying the matter. The offending LSA is thereby flushed from its scope by an immediate flooding of the routers own LSA, which must be assumed to be the correct one.

The often assumed effect of OSPF fightback is that it represents a self-healing feature which will quickly correct any erroneous route injection by an external or Byzantine node, and that thus such attacks will at most have an effect only between detection of the erroneous packet and broadcasting of the correction, at most the time interval set by the MinLSInterval.

However, as has been shown in [24], Fight Back can be counteracted by an attacker by injecting malicious packets periodically at a rate exceeding the MinLSInterval, typically 5 seconds. Indeed, Fight Back can exacerbate the effects of an attack by providing some amount of Denial-of-Service due to the potentially massive amounts of correcting packets generated by the routers for each malicious packet injected.

5.7.1 Phantom routers

Another very viable method to circumvent fightback is to emit LS Advertisements for a router that doesn't exist - a phantom router. A phantom router is normally a redundant emergency backup router set on standby in a mission-critical routing

domain to listen for instance to HELLO emits from some router, sharing its state and traffic, immediately springing into action the moment the HELLO interval is exceeded. This allows for very low latency in the case of router failure. However, since a phantom router will not participate actively, its advertisements are still valid. As such, an erroneous LSA emitted from a phantom router will persist in the LS database of the routing domain for a duration possibly far longer than the MinLSInterval - 1 hour is commonly touted as a likely worst-case scenario.

How is a phantom router set up for the purpose of network attacks? By design, OSPF routers have a relationship akin to a client-server session: packets arrive, are sent and are acknowledged, with no assumptions made at each router as to the identity and nature of the correspondent. Simply emitting a HELLO packet into an AS will immediately start the preparations for establishing an adjacency- even if this HELLO packet is emitted from for instance nemesis or ash. Whether establishing said adjacency succeeds or not is merely a question of conforming to the protocol - which can easily be done by means of automation. For all intents and purposes, routers act as oracles to each other: as long as answers conform to what is required by the protocol, adjacencies are established and maintained, and routing information is exchanged.

5.7.2 Autonomous System protected by barriers between Areas

In the case that an enemy subverts an Area Border Router linking the Area to the Backbone, the ABR could be configured to emit falsified LS Advertisements into other Areas without forwarding them into the Area of the offended router. By this means, fightback can also be circumvented.

5.8 IPSec modes and protocols for OSPFv3

OSPFv3 runs on IPv6 which, as mentioned, mandates IPSec. The exact modes and protocols to be used for OSPFv3 authentication when activated are described by RFC4552 [15], and the following section discusses these and the limitations imposed on them for this particular appliaction. Given that Link layer security services are insufficient or unsuited to providing OSPFv3 security, it follows that estimating how secure OSPF-MANET is largely depends on how well it uses IPSec security services, and thereby on the inherent properties of the IPSec protocol suite itself.

In short, ESP and Transport mode are mandatory, while AH and Tunnel mode remain optional. Authentication/Integrity are the only explicit (traffic confidentiality and replay protection are implicit) security services that are mandatory; confidentiality is optional. Whenever authentication or confidentiality are mandated, any and all OSPF packets that are not protected by AH or ESP must be discarded silently.

Note that in addition to dropping packets not conforming to the SPD set up according to RFC4552, it is assumed to be indispensable to OSPF security that ingress routers drop all incoming OSPF traffic to prevent external attacks. This is simply done by means of a rule at gateway ingress which filters at IP protocol type 89 in the IPv6 header. In the case where two IPv6 networks are connected by an IPv4 header, leading to encapsulation of the IPv6 header, gateway pre-egress admittance filtering need to be employed.

5.8.1 OSPFv3 IPSec Key Management

RFC4552 specifies key management for IPSec AH and ESP modes when used for OSPFv3.

Keying must be carried out manually; this is the only keying mechanism available to OSPFv3. The reason for why automated key distribution with IKEv1/v2 is not possible for this application, is the multicast nature of OSPF itself: when OSPF packets are sent over a broadcast interface, the sender will need to have at least two Security Associations setup individually with all recipients to achieve authentication using AH, and another two using ESP with confidentiality.

Apart from the management issue of this many Security Associations with according internal state and setup hassle, the kind of one-to-many key management would be impossible with the Diffie-Hellman-algorithm that IPSec key management relies on to establish initial keys, because this algorithm relies on the random generation of secret integers by each of the parties to the exchange.

Keys are recommended to be changed every 90 days. They must be on a numerical form, expressed hexadecimally, as ASCII keys lose crucial entropy: by limiting the available alphabet from which keys are generated, birthday attacks become exponentially easier. This especially applies in the case of manual keying, where the suggested keying interval is of such length that reasonable risk must be assumed of strong cryptanalysis efforts to uncover the key occurring. The RFC wisely forbids stream ciphers, as these would put the already duration-strained keys under additional pressure from cryptanalysis - under any circumstance, stream ciphers are not well suited for this kind of application.

5.8.2 Managing one-to-many security associations

The left hand side of figure 5.8.2 shows the fundamental problem of maintaining IPSec Security Associations (SAs) in a routing domain. Router A wishes to broadcast or multicast a routing information packet to B, C and D. However, since A must separately negotiate keys with its correspondents, and since this key negotiation requires internal state computed at each node (see Diffie-Hellmann), the security association between A and B cannot be reused between A and C. Since a two-way AH session, for instance, requires two security associations, this means that each router needs to maintain at least two SAs to every other router in its

SA database. Not the least, the advantages of broadcasting and multicasting are essentially lost, resulting in a network with vastly increased overhead: even while the contents of a flooded LSA from A will be exactly the same for B as for D, the latter cannot read it if it is sent using an SA not in its database. RFC4552 adresses this problem by demanding one ingress and one egress SA be configured manually on each router, and that each such SA is identical in terms of parameters (SPI) and keys. In other words, the SAs are static. Only by this method can IPSec currently scale on a broadcast or multicast role.

Through this measure, OSPF routers can continue to employ broadcasting and multicasting where available. To reconfigure the SAs, a rollover interval is configured, during which a third SA is used to transmit the new SA to each router by the administrator. This third SA is not pre-configured, but negotiated using IKE. An important concern is that the rekeying period should not allow unauthenticated/unencrypted packets are transmitted; thus the rollover interval, which is manually configurable. Each router will within the confines of this interval switch to the new incoming/outgoing SA set. As a consequence, the interval needs to be configured equal on all routers to assure that the rollover operation goes smoothly.

5.8.3 Other proposed keying schemes in OSPFv3

RFC4552 [15] suggests that future work could explore other key management protocols that are better suited to the broadcast environment. The protocol mentioned specifically is Kerberized Internet Negotiation of Keys/Group Secure Association Key Management Protocol (KINK/GSAKMP).

The first is one attempt at creating a dynamic keying algorithm that has a low amount of overhead. However, it still requires centralized oversight. It is specified in RFC4430 [41]. The formal basis of KINK operation is within the Kerberos concept of a Key Distribution Center. Since it has not been proposed further by the IETF as a keying algorithm for OSPFv3, this thesis does not elaborate further upon it.

5.8.4 Managing security policies

RFC4552 permits the use of one SA on several interfaces. This stems from the possibility of OSPFv3 operating multiple instances on one interface, determined by Instance ID in the OSPFv3 header. Another consequence of the multiple-instances-per-interface rule of OSPFv3 is that multiple Security Policy Databases must be supported.

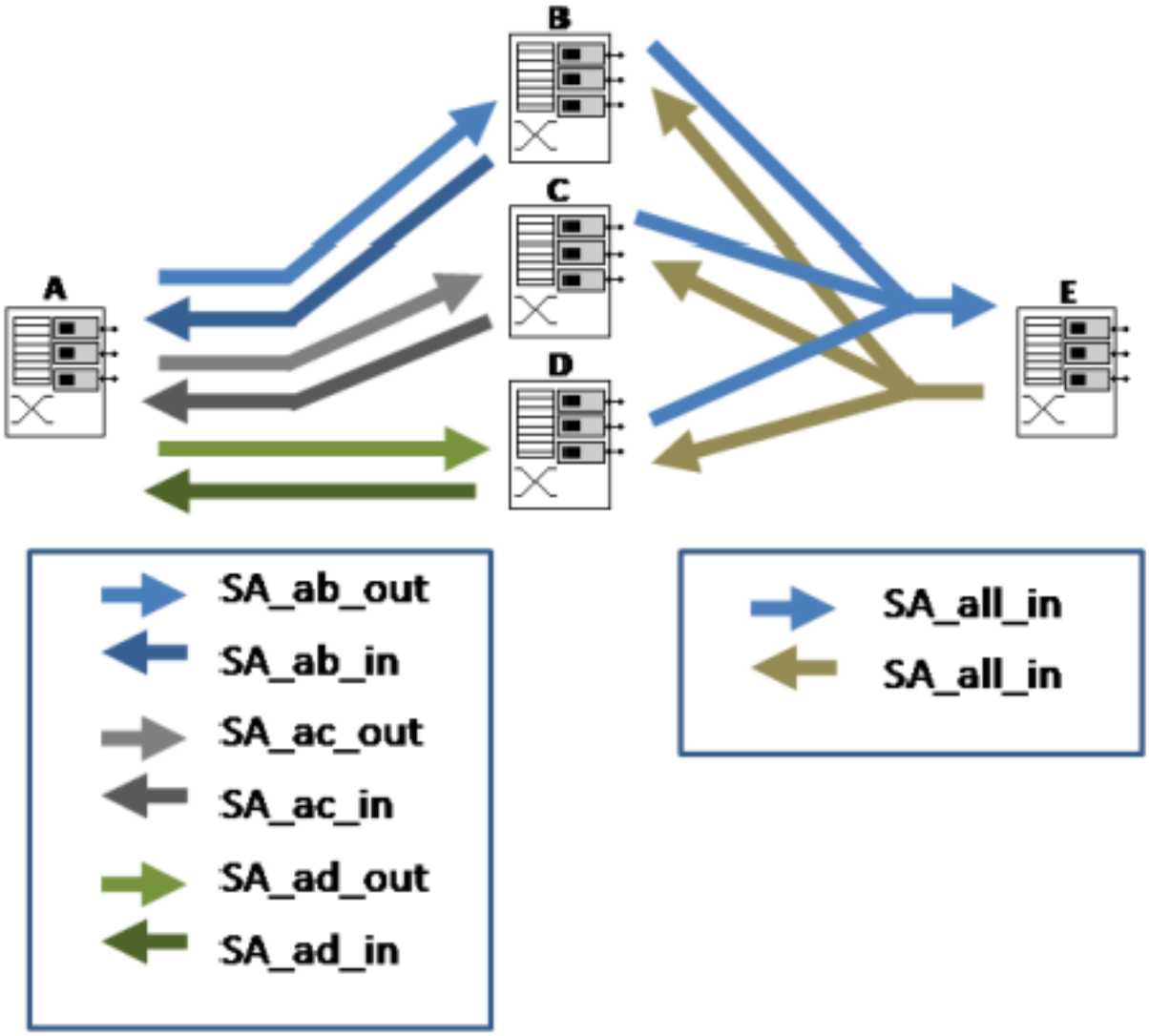

Figure 17: Illustration of Security Associations in IPSec for OSPFv3

5.9 Some reflections on OSPFv3 using IPSec in a MANET

It can be assumed that OSPF-MANET will reflect the principle of OSPFv3 of dispensing with all native authentication mechanisms in favour of IPv6 built-in IPSec.

One immediate question when considering how to offer security services to OSPF-MANET Links, is why one should not instead simply use the offered security services at the lower layer - link layer security in the shape of, for instance, 802.11i. One major point is the fact that IPSec is an end-to-end security protocol suite, whereas link-layer protocols only operate at the one-hop level. The only way to gain assurance of end-to-end integrity is to make security embed the scope of the connection, instead of being a "relay run" through the intermediate nodes. This is illustrated in Figure 18, where the thick lines describe the logical extent of the security services offered by the security protocol, while the thin line describes the session or connection. The link layer scenario at the bottom of the figure uses three link layer security "sessions", separate from each other, from host to host. The contents of the packet are available to each intermediary host. The end-to-end scenario at the top still uses the same connections, but the security "session" is now logically end-to-end and only frames and network layer headers are available to other hosts on the way. In a multi-hop environment with highly exposed nodes, this distinction becomes a concern.

Additionally, IPSec in its mandated modes for OSPFv3 could for all intents and purposes be considered the "native" security protocol for OSPFv3, and for the sake of interoperability should be retained when and where possible.

Lastly, important services such as authentication are lost in link-layer security. The main security benefit of link-layer security to MANET routing protocols, is the addition of a second layer of access control in the shape of for instance a shared key between admitted nodes. This is unfortunately not particularly useful if key management isn't MANET specific.

5.9.1 Thoughts on IPSec overhead

It has been repeatedly demonstrated that viable, effective insider attacks exist against OSPFv2 [50]. Most of these can be assumed to not affected by the minor, mainly IPv6-accomodating changes of OSPFv3; in particular, attacks using LSA injections are unaffected, since the structure of the LSA payload remains unchanged between the versions. Furthermore, all of these attacks benefit from the basic security challenges imposed by the MANET environment. However, IPSec provides a strong protection against these attacks. Can a real-life-proof OSPF-MANET implementation dispense with IPSec? If not, what degradations of performance can be expected to occur due to IPSec overhead?

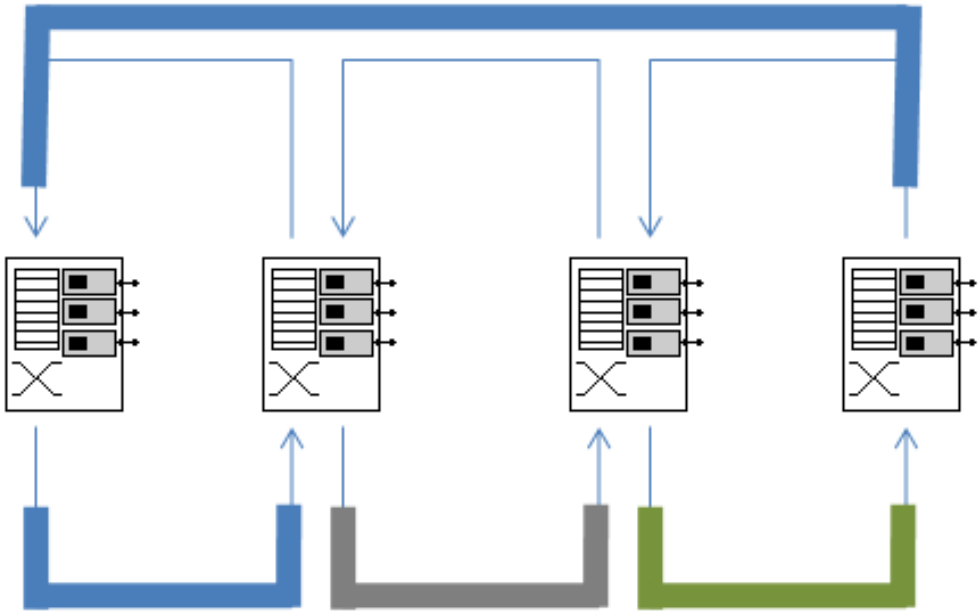

Figure 18: End-to-end vs. one-hop security

As IPSec is a key security technology in the Internet, some attention has been devoted to how much it affects performance in terms of thtoughput. IPSec performance measurement can be done using simulation or testbeds. Test scenarios usually focus on either the application (HTTP, FTP) or transport level (TCP and UDP), measuring performance using the various modes of transport and protocols (AH, ESP) in terms of throughput; notable examples are [17].

As far as OSPF is concerned, performance is mainly a function of overhead added to IP datagrams. While the comparison is not unproblematic, a good approximation of IPSec performance could be to assign some value to UDP overhead and thereby make a qualified assumption about raw IP performance under IPSec, or simply to use UDP figures in themselves. Under any circumstance, the performance issue in this context is not one of fractions, but rather of general feasibility: can a MANET routed by OSPF authenticated by IPSec even provide reasonable data rates after extra headers have taken their due?

The findings in [43] demonstrate that the performance reduction imposed by TCP vs. UDP is hidden by IPSec overhead. By this assumption, we can surmise roughly that throughput sinks to approximately half of unencrypted traffic using AH and to one third using ESP.

Keying algorithms are traffic sensitive, to the extent that their overhead exceeds that of ESP and AH traffic by around three times. Establishing key exchange sessions between a new node increases its complexity geometrically as the network size increases. The overhead caused by keying combined with

the practical difficulties of manual keying in a MANET compounds the need for an alternative keying protocol to be available to OSPF-MANET to make IPSec authentication/encryption feasible. In practice, keying IPSec according to RFC4552 becomes an issue pertaining to the "administrative" network protocol layer; while technological solutions are found to be lacking because of processing or link overhead, or because they cannot accomodate the one-to-many links, or because implementing a key infrastructure is thought to introduce single-points-of-failure, the network owner will be forced to accept the limited entropy of the manual keys and change them as he sees fit. Whether this is practical is another issue, but one which nonetheless in the end determines whether RFC4552 can offer OSPF-MANET the cryptographic protection it requires to protect itself against external node attacks.

5.9.2 The Issue of managing Security Associations in MANETs

An even more serious objection against using IPSec in MANET settings is the management of Security Associations. Since these are intended to be manual in OSPFv3, the presence of a centralized oversight to ensure this must be present in order for the IPv6 Security Header to function in a MANET. As such, the issue becomes one of management and organization. It has been claimed in [20] that a network created for the purpose of an "operational scenario" can tolerate centralization of tasks. This is because there exists a central point of trust, perhaps manifested as a command center, through which pre-configuration of security state, as an SA is a perfect example of, can be performed.

What of a network without such a central point of trust? If an ad-hoc network is to be spontaneous, it may lack any beforehand planning that could have allowed participants to agree upon security state and parameters. Works such as [19] and [13] elaborate upon key management in MANETs. The former provides a good, concise insight into the field of MANET key management.

6 Other methodology for routing security research

As most works concerning routing protocol attacks are theoretical, the extent of the damage incurred yearly by these forms of attacks is uncertain. There are far fewer reported cases of routing attacks than, for instance, DDoS attacks against applications or network intrusion. One reason for this is that routing protocols are highly complex, and attacking them warrants a high level of competence, as was the case with attacks on host security until the early nineties. One reason why host security attacks have become more common, is partially because user-friendly tools exist that permit an attacker of less competence than is required to implement such an attack with the means to perform them. Another is that host and network security attacks are becoming more motivated by the possibility of exploiting them for financial fraud or theft. These kinds tools are now gradually becoming more common, and as illicit hacker circles become gradually more aware of the obvious advantages of routing protocol attacks to enhance host and network security attacks, so will routing attacks become more of a concern. This section details the fundamental procedures and techniques that can be employed to deploy various routing protocol attacks.

This would assist to illustrate that routing attacks are indeed possible, and not just theoretical exercices, this short section shows some tools which might prove useful for the security researcher who wishes to delve further into the field. All are available through the Internet and run on any Unix equipped with the basic glibc and has Perl5 installed.

6.1 Knowing the network

The first goal of an attacker of a routing protocol is to obtain a comprehensive map of the network. To this end, several tools can be used in conjunction.

The basic tool for analyzing a network is the packet sniffer, based simply on listening to a common broadcast medium and filtering the incoming content according to rules of varying complexity, and port scanners like nmap. Packet sniffers exploit the simple broadcast link type to register any packet that comes in that is not addressed to the adapter or a broad/enabled multicast address. They are usable in routing protocol attacks to listen for routing protocol packets without actively obtaining them through queries.

The main difference between a packet sniffer and a port scanner is that the latter actively seeks out responsive interfaces on various network socket port numbers that are familiar (such as port 80 for HTTP) in order to establish which services run. While sending a Hello message into an OSPF Area does not constitute port scanning in the classic sense, it nevertheless works in the same manner. Most prudent network administrators will set rules to trigger for such behavior and set off alarms; no such thing should therefore be attempted without the consent of the network owner beforehand to prevent a false alarm.

6.1.1 nmap

`nmap` is an open-source utility that listens to IP datagrams, and parses them to obtain information about the network, and the hosts which comprise it. It is well documented, an has an active user community mainly comprising information technology security specialists, who employ nmap to audit their networks. Amongst its ample features is the possibility to detect OS versions of network hosts. At its most basic, nmap is a port scanner, but with highly advanced features to gleam the most information possible from the scans. nmap is an "active" scanner, that is, it can be heard while it scans. For instance, nmap will map TCP ports by initiating the three-way TCP handshake mechanism, then immediately close the connection once the handshake is complete and take note of the host and port number. The prudent network adminstrator will configure his Intrusion Detection to discover unsanctioned port scanning on his network, and take appropriate action as needed.

6.1.2 Siphon

Offering much of the same services as nmap, but passively, Siphon is a project which makes a network mapper which uses characteristics of various protocol implementations to extract as much information about a host originating each packet as possible. Thus, Siphon merely needs to listen for all packets on the incoming interface (promiscuous mode), without needing to reveal itself as nmap does with its active mapping.

6.2 Some tools usable for active routing attacks

Most of the routing attacks described in the routing attacks in Section 5.3 depend on the interception of routing information or routing data, followed by modification and re-insertion, or generation of new messages. Surprisingly few of the described attack types against routing protocols rely on resource-costly and difficult cryptanalysis. The reasons are of course obvious; if an attacker can dispense with costly and difficult cryptanalysis in favour of simple packet injection or leveraging other weaknesses in the basic properties of the attacked protocol, he will choose the method which provides the most result if the overall goal is simply to disrupt routing.

nemesis is a command-line utility which permits IP packets with customized headers to be injected into a network with a payload of choice. nemesis simply generates a packet based upon the command-line parameters supplied by the user, then emits it as an IP datagram. In this manner, it can for instance be used to inject packets across an adjacency that has been established by some other means. However, as it demands the user to manually create a payload (the OSPF packet, in this case), it is probably not well usable for this purpose, but rather for instance for TCP DoS attacks or similar where the payload is more or less irrelevant.

```
# ospf-ash.pl

  -- OSPF Attack Shell - 0.14 --

Using device    : eth0
Using source IP : 192.168.0.101
Using source MAC: 00:13:a9:2c:5b:a3
ash> listen
Hello from: 192.168.0.21
Found: DR : 192.168.0.22
Found: BDR: 192.168.0.21
Found: neighborList: 192.168.0.22

ash> exchange
192.168.0.22: exchange complete
192.168.0.21: exchange complete

ash> lock
ash> lsu_router('172.16.0.0','255.255.0.0')
```

Figure 19: ospf-ash usage example with route injection

Automation is key if one is to inject OSPF packets into an AS convincingly. This is where ash comes in.

ash [2], short for *Attack SHell*, is a utility which runs as an interactive shell, permitting the user to act as an OSPF instance injecting a Link State Update into the broadcast medium. ospf-ash is freely available on the Internet for download, and is written in Perl using the Net::Frame modules. It is easy to use, but warrants knowledge of the protocol to be effective. ash is notably available for OSPF, and is a highly useful tool for carrying a number of the attacks described in Section 5.3.

In Figure 19 is a usage example for ospf-ash, gathered from [2]. The shell is first used to listen for IP datagrams using protocol type 89. After a short wait, the DR and BDR respond. The user manually starts the Link State synchronization phase: DR and BDR transmit LS Database Descriptor packets to the ash session, which requests the LSAs in turn.

Once the adjacency has been built, it is maintained (locked) by periodic Hello emits. Finally, a route is injected across the adjacency from ash, in the shape of a Router LSA.

ash is not yet ported to OSPFv3. It is written in Perl using the Net::Frame module, which is well documented. The script is only 636 lines long in version

0.14, and even while it says little about the number of functions inherited through the Net::Frame module, it does demonstrate quite clearly that such tools do not need to be large and monolothic in order to be sophisticated. While not anyone could implement such a script without good knowledge of the protocol, it can be used by the less OSPF-literate since it hides much of the underlying complexity of the protocol (note for instance the "exchange" macro, which automated the LS DB exchange).

6.3 A proposal for an improved, security-accomodating network simulator

Throughout the work of this thesis, I have taken note of the methods in which routing security research is conducted. For the main part, this consists of theoretical analysis of the routing protocol, as in this thesis, or attacks are implemented in test beds using for instance vendor equipment. Notable examples of the former are mainly conducted by the hacking community, or as large-scale, long-term projects.

Simulations are a powerful tool for network researchers, permitting an indispensable tool for estimating with variable degrees of precision the effectiveness and performance of various network protocols, and also to demonstrate the functioning of technology. Network simulation tools abound; common established systems include ns2 and JSim, and more recent additions to the bestiary are GTNetS and OMNet++. All these systems are open-license, in addition, several commercial products are available. The common usage of these simulators is that of an application, a centralized event handler, which receives and emits state from different threads representing the various communicating entries present in the simulation system, notably in the case of a network, hosts, interfaces, packets, and so forth - in varying degrees of granularity depending upon modularity. The simulation is mainly deterministic; results will never be exact as pseudorandom factors will determine for instance packet emittance (the Bernoulli distribution is one typical probability distribution used for this purpose), but will generally fall within the same confines as the number of pollings increases.

The scenario to be simulated will usually be configured in some manner by the user; ns2 and JSim infamously uses Tcl scripts for this purpose, while GTNetS has a separate scenario file format and OMNet++ uses XML files. This configuration can be quite costly in terms of time, while attempts have been made to alleviate this by automating to some extent the creation of the network topology and individual node configuration.

During the simulation, the simulator writes a tracefile, which may then be used for purposes of information retrieval by graphing numerical data, parsing the text for incidences of various patterns using scripts, or even grooming the tracefile either in- or post-simulation to allow a trace visualizer show the scenario as a

graphical animated presentation. Tools of the latter category include the stand-alone *nam*, while for instance OMNet+ and GTNetS include their own visualizers.

6.3.1 Why simulations are not ideal for evaluating routing attacks

Simulators work non-interactively during simulation: the simulator registers, processes and records events and the user waits during the execution, evaluating data afterwards. This makes network simulators in their common present form less-than-ideal for the kind of research where routing protocol attacks are evaluated and tested: the lack of simulation-time monitoring prevents the observation of events related to the attack in progress that might be difficult to retrieve from post-simulation logs, or are even lost in their complexity, while the lack of in-simulation interaction prevents the researcher from introducing attack stimuli conveniently, the alternative being the often cryptic and tedious work of writing configuration files. These are by no means concerns that are important to routing security research alone; it's merely the fact that they are more important.

Contemporary simulators accomodate network researchers whose main interest lies not in the qualitative aspect of the protocol function, but rather its quantitative: how many bits per second throughput can protocol P gain from modifying parameter P_v by a given amount? Conversely, the routing security acolyte will be looking into the actual fact of a protocol being able to function. Even while Denial-of-Service is a "quantitative" attack, rather than a "qualitative" attack like the now-infamous MaxSeq++, the fact remains. This is by two observations: in the case where Denial-of-Service is instigated from outside the routing nodes themselves to overwhelm their inner event handling process by keeping incoming interfaces full, the traffic rush can easily be modelled in the proposed attack simulator without having to manually configure each and every node in the attackers' assumed botnet, and in the case where the DoS consists of the routers themselves killing a low-capacity network by being stimulated to emit increasing numbers of overhead traffic, that is again a "qualitative" response in which the researcher is mainly interested in by what stimulus in what amount at what time each router can be incited to show this destructive operating pattern. The case is simply that looking at the Bits-per-second graph afterwards hides potentially crucial details from the scientist, which might otherwise be revealed by runtime visual and numerical analysis.

While polling parameters and graphing them afterwards is principally a tool of interest for performance-oriented network research, it should by no means be discarded. However, in the proposed simulator, the polling needs to be presented graphically in runtime charts configurable by the scientist. These charts can well combine such parameters as traffic rate, key protocol variables, latency and buffer sizes.

6.3.2 Design criteria

The purpose of simulators is often stated to be to establish a credible model of reality permitting the simulator user the opportunity to experience a training scenario in which stimulus incites response; this does not immediately paralell the use of network simulators, which instead could be seen as discrete event predicters. In this sense, they resemble process controll regulators, in which for instance a refinery may introduce production-line polls of variables in order to predict the development of the system at discrete time intervals into the future in order to better tune production parameters to increase efficiency. The simulator described here would more closely resemble a simulator in the classical sense; stimulus translated, processed and responded to along the timeline.

One important feature is the way in which the system is designed. Based on modern, highly compartmentalized and modular simulators like GTNetS and OMNet++, the simulator needs to feature strong abstraction between entities like routing protocols, network interfaces, in a similar fashion as a real network node provides abstraction between the layers of the network stack. The purpose of this is mainly to offer a strong support for interchanging various modules as needed, making the replacement of one protocol for another with a similar interface seamless.

The modularity needs to be reflected in the visual representation of the simulation. While ordinary simulators mainly process the scenario in the background, which suffices perfectly fine for estimating performance and function, the attack/security simulator needs to provide a continuous, time-line graphical representation of the network. Graphical representation of tracefiles is already, as mentioned, possible with `nam`, however, this animation is only provided post-simulation. In order for the scientist to efficiently analyze the functioning of a theorized attack, the simulation must therefore respond in simulation-time.

Stimulus into the scenario can be provided by numerous means, ranging from explicitly changing variables in entities in the system on-the-fly to a more reasonable shell-type interaction. The shell used can either be proprietary, or it could, more ambitiously, be a Unix shell of any type running on top of a POSIX compliant event handler which permits the user to actually use existing applications like `nam`, `nemesis`, `snort` and similar security tools transparently, without a need for adapting them in any way. This would perhaps be the single most useful feature of this simulator. If the shell were not to be of a Unix type, an option that should under any circumstance be provided is that of at least one good, universal scripting language, preferrably perl on account of its good network modules, that would permit the user to instigate attacks more conveniently.

It would be beneficial for the simulator to allow the user to configure notifications, triggered by any given criteria. These could for instance be a given interval time between packet emittances being surpassed, or that a specific global variable in a local routing process being assigned a given value.

The simulator would need to implement security protocols at all levels. The purpose of this would not be to provide any cryptanalytic exercise value, but rather to introduce the managerial constraints of maintaining security protocols operational, mainly illustrate the complexity of key distribution, memory overhead, and management complexity. For instance, a user electing to use IPSec could choose to build a report showing the complexity of SA management in an easily presentable format. While it could be argued that such calculations are redundant as they can just as easily be carried out by pen and paper, having the option of easy presentation of them would likely be a welcome one. As before, the emphasis is on function demonstration rather than actual performance analysis.

All classes of the network, ranging from hardware-level interfaces like antennae to running processes, should be accessible in-simulation by the scientist. The main reason for this is to permit the scientist to at any time record the exact, complete state of the system: security often hides in the details, and to disclose information relevant to it, the scientist should therefore not be denied any access at all. Scripting would constitute a powerful means by which to automate information retrieval, or to evaluate it mid-simulation.

6.3.3 Benefits

It is my opinion that a simulator environment as described above, would provide network security scientists with a powerful means to analyze network and routing security theories without the excessive cost and time associated with test beds, or with circumventing or alerting network administrators of testing in a live network. While test beds are indispensable for most projects aiming for anything more than publication of findings, planning them could well be vastly more effective if scientists were able to model them beforehand and work with them in the same manner as they would with an actual network of steel, plastic and radio waves.

7 Analysis

This section aims to identify key issues in OSPF routing security when a MANET interface extension is added. In order to accomplish this, the thesis has so far focused heavily on the various protocols and more basic concepts that surround the subject. The following section, then, is devoted to tying this background into a whole.

7.1 Security and the transition from OSPFv2 to OSPFv3

The first central question is, of course, whether the transition to OSPFv3 introduces security weaknesses compared to OSPFv2. My answer to this is that it does not, or at least not to any large extent. The justifications for this statement are twofold:

First, the core OSPF state machine, which handles and stores the link state, remains essentially the same. A Shortest-Path-First algorithm operates on a set of Link State Advertisements, in the process building a routing table.

Secondly, apart from this, the Area system remains unchanged, adding the security strong and weak points of partitioning and the crucial importance of the Backbone Area, respectively. The replacement of subnets with links merely implies an extension of the former to include the entire link-layer domain on the interface.

On the other hand, security has seen at least one significant gain with the transition to the new version.

7.1.1 IPSec key management issues in a MANET

The major security breakthrough of OSPFv3 compared to v2 is without a doubt the introduction of the IPv6 Security Header (IPSec AH or ESP mode header) as mandatory, removing the somewhat ineffective [24] native OSPFv2 authentication scheme.

This act moves all cryptographic services out of the routing protocol (thereby removing the requirement for accomodating an intricate and encompassing security protocol when implementing the protocol in software - a feature of “security by simplicity”). The OSPF packet enjoys strong cryptographic security services at all levels. However, there are problems associated with using IPSec for this purpose, some of which remain unsolved. The main problem is, of course, the difficult keying issue.

Routers operate often in a one-to-many fashion. IPSec Security Associations cannot offer security services to such connections, since they are always automatically negotiated using IKE/IKEv2 on a strict one-to-one basis. Alternative keying mechanisms have been proposed that allow the creation of “group keys”,

but until then, the only supported solution is to manually configure a group SA at each router.

The answer to this problem is thereby one of moving the problem altogether into the “administrative protocol layer”, also demanding manual rekeying at regular intervals. This contradicts the distributed nature of MANETs. If OSPFv3 is to be used as a routing protocol for a MANET which :

- Is truly infrastructureless
- Is accomodating to late-entry nodes
- Has uncertain duration
- Is setup spontaneously

, then there exists a strong requirement for a keying scheme which can conform to these above demands if OSPF in a MANET that is to have these above properties. Efforts are made to uncover such a keying scheme for general use; the most comprehensive survey of such schemes at the time of writing is in [19]. No clear candidate has been identified by the author at the time of writing for replacing IKE/IKEv2 for such a role.

On the other hand, a MANET owner who intends to use the network for an operation, and is highly reliant on network and routing protocol resilience, will likely have the organizational means to carry out the stipulated manual keying method [20]. Examples of this includes the military, the police and rescue organizations, where secure channels suitable for key distribution are established as a matter of routine in the field: all these organization types possess both a clearly defined administrative organization, as well as a supply chain. This allows them points-of-trust at which trusted information can be collected. In addition, such organizations usually have experience in distributing “secure state” in some form, be it code sheets, manual programming of frequencies in radio sets or other classified information. The manual keying of a node can thereby be carried out by such an organization at any time, permitting late-entry as well as centralized keying en masse as part of preparations for bringing up the network.

Of further interest to this user category is the long timespan of the keys as seen in relation to what could be the expected lifespan of most tactical networks. A three-month recommended interval between rekeyings is a long time. There exists a good possibility that a typical operation network will be outlived by its key set.

OSPFv3 remains as vulnerable as OSPFv2 to Byzantine - or faulty node - attack vectors. An enemy striking from within can participate in the routing process unnoticeably and carefully choose a moment and method of striking using faulty packet injection. The main counterdefenses against attacks originating from this vector are sound administration policies to ensure host integrity, secure key

distribution channels, keen network observation and the possibility of adding state machines to each router permitting them to shrug off some meta-data based attacks, in particular the MaxSequence++ attack. As always, centralized administration is itself in contradiction with the idea of the entirely distributed MANET, but once more, an organization that sees a need for a resilient MANET will likely be one in which administration services, and perhaps some measure of Intrusion Detection, are a possibility; these include in particular military, police and security, and medium to major corporations.

To defend against external attacks, OSPF data must be protected en route and end-to-end; that is, even if the link (medium access) layer uses cryptographic-strength integrity and confidentiality to protect its frames, then these services must be offered at the network layer also.

This again mandates either a centralized distribution of keys for link layer or IPSec. If the link layer is unencrypted, OSPF-MANET enabled routers *must* make use of IPSec AH or ESP in the IPv6 security header as stipulated by RFC4552 in order for the routing domain to be safe from malicious packet injection as well as other attacks as described in Section 5.3.

The article at [14] shows how the existing IPSec protocol suite can be adapted for the infrastructureless constraints of a MANET, and convincingly shows that overhead is controlled, but still retains the one-to-one problem. The article is nonetheless noteworthy.

7.1.2 Throughput performance issues with IPSec

The question of whether the added packet size will affect network performance is difficult to answer. Throughput measurement is best done as a testbed exercise rather than through simulation or simple calculation. The reason is, of course, than unacceptable performance is a difficult threshold to define in a simulator, and throughput measurements in simulators rarely are very accurate. We know that OSPFv3 will generate a higher amount of control traffic or overhead traffic in all OSPF-MANET proposal candidates, and that in spite of differential Hellos there is still a higher degree of the total available bandwidth taken by OSPF in a MANET than in an ordinary wireline network.

ESP adds 50 bits of overhead to a packet. OSPF sets a maximum packet size to accomodate the smallest likely encountered MTU to avoid fragmentation and detrimental performance, according to [30] this is 1280 bits. Before deciding whether these extra 50 bits are a potential performance issue, then, some research should be done into the expected MTUs that OSPF-MANET will encounter to ensure that fragmentation does not occur.

To provide some insight into the absolute scale that can be expected, Figure 20, which was gathered from [42], shows the measured overhead imposed by IPSec in a UDP datastream running over IPv6.

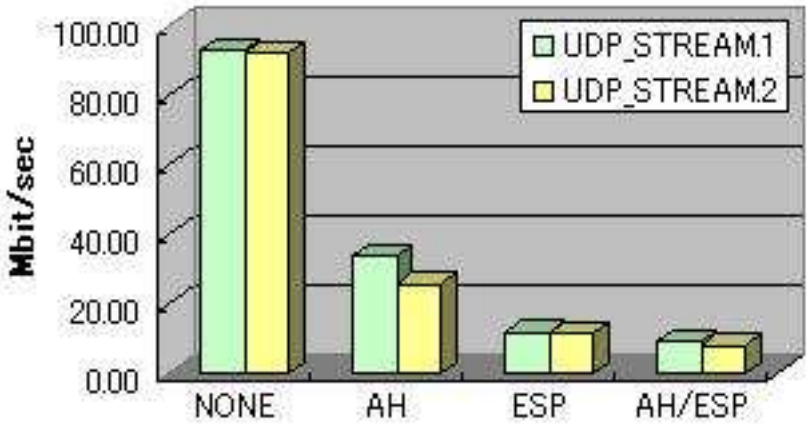

Figure 20: IPSec overhead for UDP datastream over IPv6

UDP is likely a good approximation for raw IPv6 datagrams. The figure, then provides a sense of the scale of overhead imposed by IPSec ESP and AH. The question of whether this will be detrimental to convergence properties cannot be answered without comprehensive field testing.

7.1.3 Summary of IPSec for OSPF-MANET

To conclude on IPSec: Provided IPSec can be keyed securely, and the overhead in both traffic and management is sustainable, it can offer OSPF quite strong protection against in-transit modification, and offer authentication. It can not protect against replay attacks [15], and the potential damages this can cause are documented in [24]. They include in particular DoS, as a constantly replayed Link State Request, for instance, will result in redundant database synchronization to occur, claiming resources from both routers participating in the DB exchange as well as increasing traffic in a potentially crowded wireless network. Another damaging effect that can result from such replay attacks can disrupt adjacencies between routers by falsely leading routers to believe adjacency is not accomplished, for instance.

7.2 Possible counter to the MaxSequence++ attack

The potentially devastating effect of the MaxSequence++ [49] attack has been documented by [49] [50], demonstrating how a testbed-network using vendor equipment was barred from adding LSAs to the link state for up to an hour simply by the injection of one packet with the Sequence number set to maximum. While this is an impressive result, the ingeniously simple attack methodology begs the question of whether preventing it can be done as easily.

TCP uses a sequence number scheme similar to OSPF. However, while OSPF permits out-of-order sequence numbers, simply using them to determine which of

two identical LSAs is the relevant one, TCP uses the sequence number for packet reassembly for the next layer. The TCP sequence number, unlike in OSPF, has some constraints set on it due to technical concerns. The sequence number must fit inside a *sliding window*, a configurable interval which is incremented for each arrival of a packet that has a sequence number matching the current lower boundary of the window. Any packet with a sequence number higher than what fits inside the window will be discarded.

Sliding windows are also a feature of IPSec, being the mechanism which protects against replay attacks. It is easy to see that a feature resembling the TCP sliding window state machine can be used by a router to discard packets whose sequence numbers are outside of the expected range. This feature would not interfere with the protocols operation if implemented correctly, as it would not itself modify any packets.

Instead of manually configuring or defining statically the size of the sliding window, the router process could be written so that it will accomodate a large variety of traffic scenarios by enabling it to adjust the sliding window according to the circumstances. More specifically, the sliding window state machine can use an algorithm that employs statistical distribution to establish whether a packet falls outside the *reasonably expectable* interval. Consider, for instance the statistical concept of the *outlier* - defined as any value which falls short of or exceeds the first and third quartiles (the median is the second quartile) by a distance of 1.5 times the standard deviation of the distribution. By setting the distribution to be the last 500 arrived sequence numbers, the router will adapt to the varying conditions in the network when establishing what constitutes and unreasonably high sequence number, and the process can be left automatic, aiding system administration.

While such a scheme is not mandated by the OSPF RFCs, it doesn't contradict them, either: while they specify a set of constraints inside of which an arrived packet must be found, or be dropped, nor do they prohibit any extension of packet examination as long as it does not allow non-protocol-conforming packets to be further processed by the interior SPF process. Several vendors take liberties with the existing specifications by circumventing RFC keywords (MUST, SHALL) and taking advantage of others (MAY). For instance, one vendor, Cisco, includes the ability for the network adminstrator to manually configure the Hello Interval on select models of its routers to increase network agility and responsiveness, even if the RFC specifies a standard interval: the adjustment in itself does not affect the protocol per se, it merely tunes it.

7.3 Other attacks

Black holes present a particular challenge in a MANETs, since the attackers effort to falsely obtain routes passing through his node can be aided by physical positioning unlike in an ordinary, wireline broadcast network.

The security threat to the Autonomous System as a whole is likely to increase if the MANET has a lenient admittance policy. The reason for this is that OSPF will not allow traffic from outside to enter into the AS, however, a node that has the privilege of sending out OSPF packets in a MANET can potentially inject harmful information into other Areas configured in the AS the MANET takes part in. An easy solution to this problem is to filter IPv6 protocol type 89 (OSPF) packets at the boundaries of the MANET.

The "Fightback storm" DoS-type attack will have a more severe impact on a resource-constrained MANET, as will all DoS attacks. The attacker seeking to impair the functioning of a MANET should likely therefore focus on methods to make the network "suffocate itself" by triggering massive OSPF packet emissions at strategic timing intervals.

7.4 What the MANET interface type means for OSPF security

Apart from these above-mentioned attacks, all known OSPF attacks will remain possible. What remains to be seen, however, is in what manner the increased convergence speed will counteract the effects of these attacks. Since OSPF-MANET candidates offer a more "agile" routing protocol on its interfaces, it could be conjectured that the self-healing ability of the MANET link type after a successful attack is higher than that of the traditional broadcast and point-to-multipoint link types.

Each OSPF routing process is served by a number of interfaces on various link types. It can be assumed that the security of the router as a whole will be determined by the lowest common denominator. This does not imply that a MANET-interface on a router will automatically imply a loss of security. Indeed, if the link is sufficiently weak, the simplistic point-to-point interface type can very well present a greater security risk than a MANET interface; for instance, an external attacker can have gained access to some intermediate point in the physical medium and taken control of it, modifying packets.

7.5 Concluding remarks

The thesis has extensively documented the function of OSPFv3, as well as a selection of proposals for OSPF-MANET link/interface type extension.

OSPF is a versatile, popular and well-known Internal Gateway routing protocol. The reasons for this are mainly fast convergence, an open standard, good-quality loop-free routes, versatility and scalability. It has been improved further with the latest version, in particular security is improved. Even while such OSPF aspects as the Area system add to its security, the Version 2 authentication scheme left much to be desired. For this reason, while still IPv6-only, there is some hope in the network community that version 3 will eventually be made backwards-compatible with IPv4 to reflect the slow adoption of IP version 6. This in order to benefit from the improvemed version even for todays existing IPv4 networks. Specifically, OSPFv3 benefits from good cryptographic end-to-end services in the shape of IPv6 Security Header, or equivalently, IPSec AH and ESP protocols, which provide good authentication/integrity to the entire OSPF packet, provided the necessary keying is available. OSPFv3 can be extended to function adequately in a MANET setting, although work still remains to reduce the overhead it imposes further. Still, it is able to converge and offer loop-free routes of a high quality.

The thesis then proceded to document IPSec, as well as provide a background in wireless network or MANET security issues. There is a need for improved key management for IPSec when set as a security protocol in a routing domain. More specifically, what is needed a dynamic key management scheme which would permit keying to occur across the one-to-many connections typical of routing protocols, and without manual intervention. Several proposals may provide such a service, but no standardization efforts have so far been concluded. In the meantime, manual keying in the form of manual configuration of Security Associations at each node is the required mode of operation. This may pose a problem if a network is to be truly infrastructureless or spontaneous, but can likely be circumvented when the network is an operation network that is part of a centralized organization. This is because the latter can organize points-of-trust at which keying can occur, and that such organizations often already have mechanisms in work for distribution of classified information.

OSPF resistance to Byzantine node failures, the sudden and unexpected occurrence that one node begins to exhibit non-mandated behaviour, is first and foremost implemented through strict conformance analysis of packets on arrival, dropping packets deemed outside of accepted boundaries and formalisms without any further treatment. This denies faulty state contained in Byzantine router packets from entering the state of the receiving router, in the case where the packet is malformed. If the packet is well-formed, a Byzantine router can export faulty state to other routers. Several OSPF mechanisms can be assumed to play some part in nullifying faulty state propagation. While fightback is postulated as one

such, practice shows that it often is ineffective and that it even can be used in a Denial-of-Service class of attacks.

The Designated Router scheme has security implications. The election of a router destined in the future to turn into a Byzantine node, either by a non-catastrophic logical failure or a conscious subversion by a non-authorized entity, as Designated Router in an OSPF Area will essentially mean that all routers in the Area will be adjacent to a faulty router and assume its state through periodic updates. All state arriving at the faulty router must be assumed to be untrustworthy in such a scenario, and consequently all adjacencies must be considered tainted. This is a dramatic, if extreme, example of how the DR scheme potentially can introduce a Single-point-of-Failure weakness in an OSPF network - even if the DR is Byzantine in nature, the BDR will not assume its duties until Hellos from the DR subside.

The OSPF Area system is a security benefit. However, the introduction of one or more routers with a MANET interface enabled into an AS may be a security liability, as the inherent security threats of the more exposed link type potentially can trickle into the Autonomous System. OSPF can easily be secured from most outsider attacks by filtering IP frames with protocol type 89 at network ingress, as is also usually done. However, the inclusion of a MANET Area into an existing OSPF network can constitute a backdoor into the AS since the general medium will be available to would-be attackers, though disadvantaged by the need for geographic proximity.

MANET wireless networks face a number of security challenges imposed by their limited capacity, mobility, general access medium and lack of centralized infrastructure. These include a vulnerability to attacks carried out from external nodes, to difficulties in achieving cryptographic keying. MANET security has become a concern for numerous research projects which aim to introduce these networks to a wider usage than currently, as their potential benefits of resilience, generality and mobility or considered highly desirable. While secure routing protocols have been proposed for MANET networks, OSPF is not such a secure protocol by inherent design and needs to have security retrofitted. Even though it has been demonstrated that IPSec is not optimal for this, there are still strong advantages of using it, including interoperability and the good ability it has for extension of protocols. It offers generally good cryptographic algorithms, but the hash algorithms do need some attention, as in particular SHA-1 has been subject to substantial cryptanalysis efforts in later years.

The thesis has presented some useful utilities that could be used by a routing protocol attacker, including an automated tool that allows a user to interactively build adjacencies and inject LSAs. Further work is possible in the field of routing attack research, and while simulations and testbeds provide a method of observing such attacks in practice, an application was suggested which extends current network simulators with the capability of interaction during the simulation run.

Such an application would have a lessened emphasis on raw throughput and instead focus on the state of the routers and the operation of the routing protocol. This could make implementing a potential attack far easier in order to verify its validity without going through costly testbeds and with better ability to control the attack than with a non-interactive, scripted simulator.

When the OSPF-MANET working group finally arrives at a candidate for interface type extension, OSPFv3 will be a highly versatile routing protocol suitable for almost any link type. In spite of this, security constraints in the MANET network type further expose the challenging task of using IPSec as end-to-end security for OSPF. Further work into the field should therefore focus on how IPSec modes and operation for OSPF can be improved. Work has been and is being done on MANET key management, and what has been done in this field can possibly be of interest to OSPF security researchers.

8 Terms and definitions

Most of these definitions are directly the same as used in most of RFC2460 and RFC1930. For reasons of clarity I also include some central terms I use.

- Upper layer - a protocol layer immediately above IPv6. Examples are transport protocols such as TCP and UDP, control protocols such as ICMP, routing protocols such as OSPF, and internet or lower-layer protocols being "tunneled" over (i.e., encapsulated in) IPv6 such as IPX, AppleTalk, or IPv6 itself [11]
- Node - any device (router or host) that implements IP.
- Router - a node that forwards IP packets not explicitly addressed to itself.
- Host any node that is not a router, i.e. it does not forward packets addressed to others.
- Link - A communications facility at a layer below IP, over which nodes exchange IP packets directly without decrementing IP TTL (Hop Limit).
- Neighbors - nodes attached to the same wired medium link, or nodes which are within two-way or one-way transmission and/or listening range on the wireless medium link. (See Note below.)
- Interface - a node's attachment to a link.
- Address - an IPv6-layer identifier for an interface or a set of interfaces.
- Packet - an IPv6 header plus payload.
- General - capable of operating in a general capacity; common; not particular.
- Dedicated - set apart for a specific purpose alone.
- Autonomous System (AS) - a connected group of one or more IP prefixes run by one or more network operators which has a *single* and *clearly defined* routing policy.
- Router adjacency - that a set of two or more routers implementing a Link State routing protocol have synchronized their link state databases with each other. A distinction of particular importance is that adjacency does not imply neighborship, and vice versa.
- Connected (graph theory) - a path can be established from every vertice v to all other vertices in the graph.

- Dominating set (graph theory) - the subset *G' = (E', V')*of the graph *G = (E, V)* such that for every vertex in *V* that is not also a member of *V'*, there exists an edge between itself and some vertex in *V'*. A colloquial term sometimes used for the dominating set is the "backbone" of the graph.

Note : the definition of 'neighbors' needs to be broadened for topics in the wireless medium, to imply the possible one-way or two-way links that may be encountered.

8.1 Abbreviations

- ABD - Area Border Router (OSPF)
- AODV - Ad-hoc On-demand Distance Vector
- AOR - Active Overlapping Relay
- AS - Autonomous System
- ASBR - AS boundary router(OSPF)
- (B)DR - (Backup) Designated Router(OSPF)
- DH - Diffie-Hellman
- IETF - Internet Engineering Task Force
- IGP - Interior Gateway Protocol
- IP - Internet Protocol
- LSA - Link State Advertisement
- LSU - Link State Update
- LSDB - Link State Data Base
- KINK - Kerberized Internet Negotiation of Keys
- MANET - Mobile Ad-hoc NETwork
- (B)MDR - (Backup) Mobile Designated Router
- MPR - Multi Point Relay
- NSSA - Not-so-stubby Area(OSPF)
- OLSR - Optimized Link-State Routing
- OSPF - Open Shortest Path First(OSPF)
- OSPF-MDR - OSPF Mobile Designated Router

- RFC - Request For Comments (an IETF technical standards document)
- SA - Stubby Area(OSPF)
- TSA - Totally Stubby Area(OSPF)
- TLV - Type/Length/Value
- WOSPF-OR - Wireless OSPF Overlapping Relays
- SA - Security Association
- SHA - Secure Hash Algorithm
- SPD - Security Policy Database

References

[1] J. Ahrenholz, T. Henderson, P. Spagnolo, E. Baccelli, T. Clausen og P. Jacquet. Ospfv2 wireless interface type, 2005. INTERNET DRAFT expired Nov 2005 draft-spagnolo-manet-ospf-wireless-interface-01.txt.

[2] Patrice Auffret. Ospf attack shell (ash).

`http://www.gomor.org`

[3] E. Baccelli, D. Nguyen, P. Jacquet og T. Clausen. Ospf mpr extension for ad hoc networks, februar 2007. INTERNET-DRAFT draft-baccelli-ospf-mpr-ext-03.

[4] A. Barbir, S. Murphy og Y. Yang. Generic Threats to Routing Protocols. RFC 4593 (Informational), oktober 2006.

[5] Steven M. Bellovin. Security problems in the tcp/ip protocol suite. *Computer Communication Review*, 19(2):32–48, april 1989.

[6] Levente Buttyán og István Vajda. Towards provable security for ad hoc routing protocols. I *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, side 94–105, New York, NY, USA, 2004. ACM Press. ISBN 1-58113-972-1.

[7] Christophe De Cannière og Christian Rechberger. Finding sha-1 characteristics: General results and applications. *Advances in Cryptology Ž2013 ASIACRYPT 2006*, side 1–20, 2006.

[8] M. Chandra. Extensions to ospf to support mobile ad-hoc networking, januar 2007. INTERNET-DRAFT draft-chandra-ospf-manet-ext-04.

[9] T. Clausen og P. Jacquet. Optimized Link State Routing Protocol (OLSR). RFC 3626 (Experimental), oktober 2003.

[10] R. Coltun, D. Ferguson og J. Moy. OSPF for IPv6. RFC 2740 (Proposed Standard), desember 1999.

[11] S. Deering og R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460 (Draft Standard), desember 1998.

[12] D. Dolev og A. Yao. On the security of public encryption protocols. *IEEE Transactions on Information Security*, 29(2):198–208, 1983.

[13] K. Fokine. Key management in ad hoc networks. Hovedfagsoppgave, Lindköpings tekniska högskola, 2002.

[14] Abhrajit Ghosh, Rajesh Talpade, Moncef Elaoud og Michael Bereschinsky. Securing ad-hoc networks using ipsec. *Military Communications Conference, 2005. MILCOM 2005. IEEE*, 5:2948– 2953, 2005.

[15] M. Gupta og N. Melam. Authentication/Confidentiality for OSPFv3. RFC 4552 (Proposed Standard), juni 2006.

[16] S. Gupte og M. Singhal. Secure routing in mobile wireless ad hoc networks. *Ad Hoc Networks*, 1:3, 2003.

[17] George Hadjichristofi, Nathaniel Davis og Scott Midkiff. Ipsec overhead in wireline and wireless networks for web and email applications. *Proceedings of the IEEE*, side 543–547, april 2003.

[18] D. Harkins og D. Carrel. The Internet Key Exchange (IKE). RFC 2409 (Proposed Standard), november 1998. Obsoleted by RFC 4306, updated by RFC 4109.

[19] Anne Marie Hegland. Survey of key management in ad-hoc networks. *IEEE Communications Surveys & Tutorials*, 8(33):48–66, 2006.

[20] Anne Marie Hegland. *Towards reliable Network Services in ad hoc Routing protocols: Protecting the Routing Protocols*. Doktorgradsoppgave, University of Oslo, 2007.

[21] Thomas R. Henderson, Phillip A. Spagnolo og Guangyu Pei. Evaluation of ospf manet extensions (boeing technical report), juli 2005.

[22] Kenneth Holter. Wireless extensions to ospf: Implementation of the overlapping relays proposal. Hovedfagsoppgave, University of Oslo, 2006.

[23] Dijiang Huang, A. Sinha og D. Medhi. On providing confidentiality in link state routing protocol. *Consumer Communications and Networking Conference*, 2:671 – 675, January 2006.

[24] E. Jones og O. LeMoigne. Ospf security vulnerabilities analysis, juni 2006. INTERNET-DRAFT Expired Draft draft-ietf-rpsec-ospf-vuln-02.txt.

[25] C. Kaufman. Internet Key Exchange (IKEv2) Protocol. RFC 4306 (Proposed Standard), desember 2005.

[26] S. Kent. IP Authentication Header. RFC 4302 (Proposed Standard), desember 2005.

[27] S. Kent. IP Encapsulating Security Payload (ESP). RFC 4303 (Proposed Standard), desember 2005.

[28] D. Maughan, M. Schertler, M. Schneider og J. Turner. Internet Security Association and Key Management Protocol (ISAKMP). RFC 2408 (Proposed Standard), november 1998. Obsoleted by RFC 4306.

[29] Johann Van Der Merwe, Dawoud Dawoud og Stephen McDonald. A survey on peer-to-peer key management for mobile ad hoc networks. *ACM Comput. Surv.*, 39(1):1, 2007. ISSN 0360-0300.

[30] J. Moy. *OSPF - Anatomy of an Internet routing protocol*. Addison-Wesley, 1998.

[31] J. Moy. OSPF Version 2. RFC 2328 (Standard), april 1998.

[32] Keng Seng Ng og Seah W.K.G. Routing security and data confidentiality for mobile ad hoc networks. *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*, 3:1821–1825, April 2003.

[33] P. Nikander, J. Kempf og E. Nordmark. IPv6 Neighbor Discovery (ND) Trust Models and Threats. RFC 3756 (Informational), mai 2004.

[34] R. Ogier og P. Spagnolo. Manet extension of ospf using cds flooding, mars 2006. INTERNET-DRAFT draft-ogier-manet-ospf-extension-07.txt.

[35] Richard Ogier. Advantages of ospf-mdr, februar 2006. INTERNET-DRAFT draft-ogier-ospf-mdr-position-00.txt.

[36] A. Patcha og A. Mishra. Collaborative security architecture for black hole attack prevention in mobile ad hoc networks. *IEEE Procedings of RAWCON '03*, side 75–78, 2003.

[37] C. Perkins, E. Belding-Royer og S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561 (Experimental), juli 2003.

[38] Radia Perlman. *Network layer protocols with Byzantine robustness*. Doktorgradsoppgave, Massachusetts Institute of Technology, 1988.

[39] D. Piper. The Internet IP Security Domain of Interpretation for ISAKMP. RFC 2407 (Proposed Standard), november 1998. Obsoleted by RFC 4306.

[40] Eric C. Rosen. Vulnerabilities of network control protocols: An example. RFC 789, 1981.

[41] S. Sakane, K. Kamada, M. Thomas og J. Vilhuber. Kerberized Internet Negotiation of Keys (KINK). RFC 4430 (Proposed Standard), mars 2006.

[42] Ariga Seiji, Nagahashi Kengo, Minami Masaki, Esaki Hiroshi og Murai Jun. Performance evaluation of data transmission using ipsec over ipv6 networks.

`http://isoc.org/inet2000/cdproceedings/1i/1i_1.htm`

[43] Ariga Seiji, Nagahashi Kengo, Minami Masaki, Esaki Hiroshi og Murai Jun. Performance evaluation of data transmission using ipsec over ipv6 networks. *Inet Japan*, juli 2000.

[44] Ling Shi. Implementing wireless extensions for ospf in j-sim. Hovedfagsoppgave, University of Oslo, 2007.

[45] R. Shirey. Internet Security Glossary, Version 2. RFC 4949 (Informational), august 2007.

[46] P. Spagnolo og T. Henderson. Comparison of proposed ospf manet extensions. *Military Communications Conference (MILCOM) 2006*, oktober 2006.

[47] Douglas R. Stinson. *Cryptography - Theory and Practice*. Chapman&HallCRC, third utgave, 2006.

[48] B. Vetter, F. Wang og S. Wu. An experimental study of insider attacks on the ospf routing protocol. *IEEE ICNP*, 1997.

[49] B. Vetter, F. Wang og S. F. Wu. An experimental study of insider attacks for ospf routing protocol. I *ICNP '97: Proceedings of the 1997 International Conference on Network Protocols (ICNP '97)*, side 293, Washington, DC, USA, 1997. IEEE Computer Society. ISBN 0-8186-8061-X.

[50] F. Wang og S. Wu. On the vulnerabilities and protection of ospf routing protocol. *IEEE ICNP*, 1998.

[51] Xiaoyun Wang, Yiqun Lisa Yin og Hongbo Yu. Finding collisions in the full sha-1, 2005.

[52] H. Yang, H. Luo, H. Ye, S. Lu og Zhang L. Security in mobile ad-hoc networks: Challenges and solutions. *IEEE WIreless Communications*, februar 2004.

[53] L. Zhou og Z. Haas. Securing ad hoc networks. *IEEE Network*, side 24–30, november 1999.